ASSESSING THE COMPETING CHARACTERISTICS OF PRIVACY AND SAFETY WITHIN VEHICULAR AD HOC NETWORKS

THESIS

Jacob W. Connors

AFIT-ENG-MS-18-M-019

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-18-M-019

ASSESSING THE COMPETING CHARACTERISTICS OF PRIVACY AND SAFETY WITHIN VEHICULAR AD HOC NETWORKS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Jacob W. Connors, B.S.

March 2018

AFIT-ENG-MS-18-M-019

ASSESSING THE COMPETING CHARACTERISTICS OF PRIVACY AND SAFETY WITHIN VEHICULAR AD HOC NETWORKS

Jacob W. Connors, B.S.

Committee Membership:

Dr. Scott R. Graham
Chair

Dr. Scott L. Nykl
Member

Lt Col Logan O. Mailloux, PhD
Member

Abstract

The introduction of Vehicle-to-Vehicle (V2V) communication has the promise of decreasing vehicle collisions, congestion, and emissions. However, this technology places safety and privacy at odds; an increase of safety applications will likely result in the decrease of consumer privacy. The National Highway Traffic Safety Administration (NHTSA) has proposed the Security Credential Management System (SCMS) as the back end infrastructure for maintaining, distributing, and revoking vehicle certificates attached to every Basic Safety Message (BSM). This Public Key Infrastructure (PKI) scheme is designed around the philosophy of maintaining user privacy through the separation of functions to prevent any one subcomponent from identifying users. However, because of the high precision of the data elements within each message this design cannot prevent large scale third-party BSM collection and pseudonym linking resulting in privacy loss. In addition, this philosophy creates an extraordinarily complex and heavily distributed system. In response to this difficulty, this thesis proposes a data ambiguity method to bridge privacy and safety within the context of interconnected vehicles. The objective in doing so is to preserve both Vehicle-to-Vehicle (V2V) safety applications and consumer privacy. A Vehicular Ad-Hoc Network (VANET) metric classification is introduced that explores five fundamental pillars of VANETs. These pillars (Safety, Privacy, Cost, Efficiency, Stability) are applied to four different systems: Non-V2V environment, the aforementioned SCMS, the group-pseudonym based Vehicle Based Security System (VBSS), and VBSS with Dithering (VBSS-D) which includes the data ambiguity method of dithering. By using these evaluation criteria, the advantages and disadvantages of bringing each system to fruition is showcased.

Acknowledgments

I would like to acknowledge my fellow classmates for their unrelenting support and motivation. I would also like to thank Dr. Scott Graham, my advisor, for his incredible insight and counsel over this research thesis. I would also like to thank my peers at the Air Force Metrology & Calibration Center to allow me this academic opportunity. Lastly, I would like to thank my family; for without their encouragement and support I would not be the person I am today.

Jacob W. Connors

Table of Contents

Page

Page

List of Figures

List of Tables

List of Acronyms

Abbreviation Page

ACC Adaptive Cruise Control . . . 19

AES-CCM Advanced Encryption Standard in Counter Mode with Cipher Block Chaining Message Authentication Code . . . 14

AIFS Arbitration Inter-Frame Space . . . 8

ADSB Automatic Dependent Surveillance–Broadcast . . . 40

BSM Basic Safety Message . . . 78

CA Certificate Authority . . . 7

CA Certificate Authority . . . 7

CACC Cooperative Adaptive Cruise Control . . . 19

CRL Certificate Revocation List . . . 12

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance . . . 8

CVSS Common Vulnerability Scoring System . . . 79

ECDSA Elliptic Curve Digital Signature Algorithm . . . 14

ECIES Elliptic Curve Integrate Encryption Scheme . . . 14

EDCA Enhanced Distributed Channel Access . . . 8

EEBL Emergency Electronic Brake Light . . . 33

FAA Federal Aviation Administration 40

FCC Federal Communication Commission 6

FCW Forward Collision Warning 33

IM Intersection Manager 59

IMA Intersection Motion Assist 33

IPv6 Internet Protocol version 6 10

ITS Intelligent Transportation System 6

LLC Logical Link Layer 10

MAC Medium Access Control 8

NHTSA National Highway Traffic Safety Administration 78

OBU On-Board Unit 70

P2PCD Peer-to-Peer Certificate Distribution 13

PDU protocol data unit 13

PHY physical 8

PKI Public Key Infrastructure 78

RSU Road Side Unit 82

ASSESSING THE COMPETING CHARACTERISTICS OF PRIVACY AND SAFETY WITHIN VEHICULAR AD HOC NETWORKS

I. Introduction

Over the course of the past century, innovations in technology have increased vehicle safety. Innovations such as seat belts, airbags, and vehicle design architecture have all improved occupant safety in the event of a vehicle-on-vehicle collision. However, there is a physical limitation to these mechanisms. These safety devices are reactive; designed to protect a vehicle's occupants *after* a collision has occurred. What if a driver could be alerted *before* a collision in order to prevent it from occurring?

Vehicle-to-Vehicle (V2V) communication has set out to create a safety proactive vehicular environment. By broadcasting information such as speed, heading, location, and other safety-critical information vehicles would be capable of alerting drivers of hazardous scenarios. However, with the disclosure of information, consumer privacy is at risk and needs to be addressed before V2V communication can deployed within production vehicles.

1.1 Background and Motivation

The National Highway Traffic Safety Administration (NHTSA), the U.S. government agency responsible for addressing safety concerns have been at the forefront of V2V communication. In early 2017, NHTSA published a Notice of Proposed Rulemaking (NPR) that presents an overview of the V2V technology, logistical impacts, and the schedule of the proposed implementation timeline [1]. Much of the work within this thesis is based of information within the 2017 NHTSA NPR.

The environment that V2V communication creates is referred to as a Vehicular Ad-Hoc Networks (VANETs). The different types of devices that constitute a VANET are On-Board Units (OBUs) and Road Side Units (RSUs). V2V is the communication of two OBUs while the communication of vehicles and RSUs is referred to as vehicle-to-infrastructure (V2I) communication. Vehicle-to-Anything (V2X) represents communication between a vehicle and anything else that is not an OBU or RSU. The purpose of RSUs is to issue security credentials, relay traffic environment conditions, and communicate to higher level certificate authorities. OBUs transmit Basic Safety Messages (BSMs) at a frequency of 10 Hz with typical transmission range of three hundred meters. The data within these messages allows for applications such as forward collision warning, blind spot warning, and electronic emergency brake lights and similar applications [1].

NHTSA is invested in protecting the privacy of the consumer. The current leading Public Key Infrastructure (PKI) scheme, the Security Credential Management System (SCMS), is modeled around a "privacy by design" approach [1]. This design calls for a complex PKI that protects consumer privacy from insider threats within the SCMS, however, it does little to hinder outsider threats. NHTSA states V2V messages shall not include "data directly identifying a specific private vehicle or individual regularly associated with it, or data reasonably linkable, as a practical matter, to an individual." By issuing this decree, information such as vehicle identification number, license plate number, and other unique data is prohibited from being transmitted. However, other information such as location, speed, and temporary identification numbers are allowed. BSM linking – connecting one or more BSMs to an individual vehicle – will be possible through the use of these BSM contents and data from other sources.

1.2 Problem Statement

The introduction of smart devices, such as V2V, has the promise of increasing convenience, safety, and overall quality of life. However, with the increase of technology, this can lead to malicious actors and unwanted disclosure of information. Nonetheless, V2V safety capabilities rely on the willful disclosure of information from the majority of vehicles on the road. This creates a predicament for drivers who want to maintain privacy (i.e., not broadcast location information), but still obtain the added safety benefits of V2V. The trade-off between safety and privacy in a V2V environment can be summarized by the following: safety is heightened through the disclosure of information and privacy is heightened through the retention of information. This thesis explores the current V2V privacy loss mitigation schemes and strikes a meaningful balance between the contrasting natures of safety and privacy in a V2V environment by introducing data ambiguity techniques to increase the sophistication required to track vehicles.

1.3 Research Objectives

In order to properly understand, develop, and analyze V2V privacy, the following objectives are specified:

- Understand the workings of Wireless Access in Vehicular Environments (WAVE): the protocol that makes V2V possible. This includes understanding what information is sent with each message and how a vehicle utilizes it.
- Understand the proposed certificate management systems that allow each vehicle to sign and verify.
- Understand privacy from a legal standpoint in order to properly evaluate privacy within a V2V environment.

- Obtain NHTSAs perspective on V2V to better understand the current state of V2V research and legislation.
- Develop a data ambiguity solution to balance privacy and safety proof of concept.
- Evaluate the solution versus current schemes and report effectiveness.
- Introduce policies to thwart point of origin and destination information disclosure.
- Analyze the realistic expectation of privacy within the Information Age.

The fulfillment of these objectives allows for V2V communication safety applications and permits only safety-critical information to be collected by third-parties. In doing so, this improves consumer privacy by increasing the level of technical ability required to link V2V messages to a specific vehicle .

1.4 Approach

The approach this thesis takes is a mostly qualitative perspective. The use of statistical analysis is not yet applicable as this work focuses on the projected disclosure of information and its effects. The constraints surrounding time, resources, and safety has driven the methodology decisions concerning V2V message broadcast simulation. The analysis of the effects on consumer privacy and safety rely on a deep understanding of the technology because V2V has not been widely adopted nor mandated as of the writing of this document. In addition to a qualitative analysis, a quantitative analysis is also presented through the use of the Common Vulnerability Scoring System (CVSS) for assigning scores to systems in relation to disclosing consumer information.

1.5 Organization

This document is broken into five chapters and the remaining four chapters are described below:

Chapter II introduces the WAVE protocol and its components and operation parameters. Information exchanged with each V2V message is presented and discussed. Applications that use this information is presented to highlight the safety benefits possible through V2V communication. A privacy law taxonomy and its relevancy to V2V is presented in order portray a comprehensive definition of privacy and introduce topics utilized in analysis. Lastly, research conducted by NHTSA is presented to portray current perspectives of V2V communication.

Chapter III introduces the research methodology of BSM linking. The three PKI schemes under analysis are presented along with how BSM transmission is emulated in a simulation environment. The data ambiguity method of dithering is presented and defined.

Chapter IV introduces the analysis of the topics presented. Implications of each scheme are discussed along with the safety impacts of dithering. The BSM linking algorithms for each scheme are presented through the use of flowcharts. A VANET Metric Classification is presented and discussed in accordance with each PKI scheme discussed along with a non-VANET analysis to provide a viewpoint of current technology. Lastly, policies are presented to reduce individual privacy loss.

Chapter V concludes the document by summarizing the discussions, the findings presented, areas of future work, and contributions. The difficulties discovered within this topic are discussed. Opinions of the author are presented regarding the future of V2V communication will become as the technology develops.

II. Background and Related Research

The purpose of this chapter is to provide a technical summary of the Wireless Access in Vehicular Environments (WAVE) protocol which is the underlying technology of Vehicle-to-Vehicle (V2V) communications [2]. In addition, this chapter discusses current research within V2V privacy and each individual WAVE component necessary for operation is discussed. Each element of the Basic Safety Message (BSM) is highlighted to showcase the information being transmitted between V2V devices. Next, V2V safety applications are presented to show the functionalities that are made possible by V2V. The two candidate Public Key Infrastructure (PKI) systems, Security Credential Management System (SCMS) and Vehicle Based Security System (VBSS), are presented for back end security management. Research conducted by the National Highway Traffic Safety Administration (NHTSA) is presented which discusses past BSM linking research, misbehavior detection techniques, and NHTSA's V2V Privacy Impact Assessment [1],[3]. In addition, three privacy preservation methods are discussed. Finally, this chapter concludes with a taxonomy on privacy law. This showcases the impact V2V could have on consumer rights if V2V becomes mandated.

2.1 WAVE Overview

In 1999, the Federal Communication Commission (FCC) allocated 75 MHz for V2V communication within the 5.850 - 5.925 GHz band [4]. The FCC's motivation was to facilitate implementations of Intelligent Transportation Systems (ITSs) to decrease roadway congestion, increase passenger safety, and reduce the use of fossil fuels. Using the guidelines set by the FCC the IEEE 1609 Working Group created the IEEE 1609 Family of Standards for WAVE, with the intent to allow vehicles to communicate wirelessly and securely[2]. These items together create what is referred

to as a Vehicular Ad-Hoc Network (VANET).

2.1.1 Operation.

The WAVE standard operates on two types of hardware:

1. On-Board Units (OBUs) are the WAVE boxes installed within each vehicle.
2. Road Side Units (RSUs) are any stationary object that has a WAVE-capable device installed.

As a vehicle travels, the OBU receives and transmits information from RSUs along its route. This information could include anything from roadway delays to certificate renewals from a Certificate Authority (CA). OBUs can also connect to other OBUs to share safety messages and other critical data. RSUs could be traffic lights, light poles, and other road side objects and infrastructure. They are typically stationary, but it is possible for a RSU to be transportable when the case calls for it (e.g. construction, law enforcement discretion, and accidents) [5].

Figure 1 depicts the WAVE protocol stack. The following sections will discuss each individual standard and its role within a VANET.

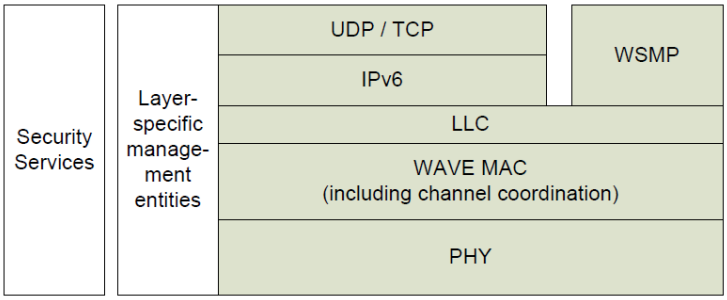

Figure 1. WAVE protocol stack diagram.

2.2 IEEE 802.11p

IEEE 802.11p covers the physical (PHY) and Medium Access Control (MAC) layers of the WAVE protocol. This standard incorporates aspects from the IEEE 802.11a standard. This is done to prevent rewriting a ubiquitous wireless PHY layer design. However, there are three modifications that cater to the mobile WAVE environment. The first change IEEE 802.11p incorporates is the configuration to operate within 10 MHz wide channels whereas a typical 802.11a channel is 20 MHz. This allows for longer guard intervals (discussed in 2.4) which helps prevent interference. IEEE 802.11p introduces improved receiver requirements to reduce cross channel interference present in 802.11 devices as well as improved transmission masks [6].

The MAC layer utilizes Enhanced Distributed Channel Access (EDCA) which relies on Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) to transmit packets across the network. In CSMA/CA, a node will observe the network and will transmit only if the network is open for a certain length of time - called the Arbitration Inter-Frame Space (AIFS). Otherwise, the node backs off for a random amount of time before attempting to transmit again. CSMA/CA is optimal for a WAVE environment because altering the AIFS allows for packet priority when transmitting. High priority (such as safety messages) packets will have the shortest AIFS while lower priority packets (non-safety messages) will have longer AIFS times [7].

2.3 IEEE 1609.4 - Multi-Channel Operation

The IEEE 1609.4 protocol operates on top of IEEE 802.11p. The purpose of this standard is to create a seamless data transfer through multiple channels from the lower physical layer to upper layers of the WAVE protocol. There are seven 10MHz channels: one Control Channel (CCH) and six Service Channels (SCHs) of which two are reserved (see Figure 2). The CCH broadcasts critical safety messages as well as

available service announcements while the SCHs are utilized by those services. The key difference between the CCH and SCHs is that the CCH only permits data frames containing WAVE Short Message Protocol (WSMP) messages; whereas the SCHs permit both WSMP messages and IPv6 messages [8].

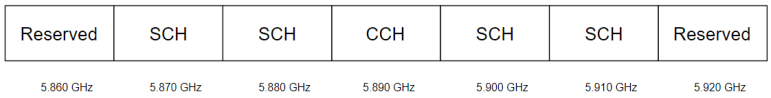

Figure 2. Seven channels dedicated for WAVE use.

A device can gain access to the CCH or SCHs in one of three ways:

1. Continuous access: The channel (either CCH or SCH) is available for an unrestricted amount of time.

2. Immediate access: A device switches to a new channel immediately for an unrestricted amount of time.

3. Alternating access: A device switches between CCH and SCH for a specified time interval.

Alternating access is the common access method utilized amongst WAVE devices. Access is granted for specific time intervals. The different time intervals are listed below:

1. Time interval: specified to be one 50 ms channel allocation (CCH or SCH).

2. Sync Interval: Two adjacent time intervals utilized for synchronization (100 ms).

3. Guard interval: At the beginning of each time interval; are used to account for radio effects and inaccuracies when switching channels (4 - 6 ms).

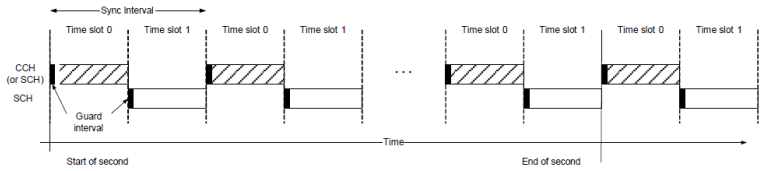

Figure 3. Alternating access diagram showcasing each time interval.

A guard interval is split into three sections. The first and third section are determined by half the synchronization tolerance. The second is determined by the maximum channel switching time allowed. Data transmissions are prohibited during a guard interval because a device could still be in-between channels. Thus, at the beginning of a guard interval all transmissions on the current channel are suspended and transmissions on the new channel begin once the guard interval ceases. When a device switches during the guard interval, it declares the medium busy to prevent simultaneous transmissions [8]. A 100 ms Sync interval maps directly to the 10 MHz frequency rate specified in IEEE 802.11p [9].

2.4 IEEE 1609.3 - Network Services

IEEE 1609.3 provides the functionality to process data across the WAVE protocol stack and consists of network and transport services. At the very minimum, a WAVE device must have incorporated the following features:

1. Logical Link Layer (LLC) sublayer: Identifies higher layer protocol to be utilized.

2. WAVE Short Message Protocol (WSMP): Protocol unique to WAVE that deliver WAVE Service Advertisements (WSAs) and WAVE Short Message (WSM) to higher layers.

3. Internet Protocol version 6 (IPv6): Support for protocols such as UDP and/or TCP.

4. The ability to transmit and/or receive.

Note: WAVE devices can support WSMP, IPv6, or both.

The LLC header contains a 2-octet *EtherType* field that designates what particular protocol is to be used. When the LLC receives a transmission request from IPv6 or WSMP, it sets the value *EtherType* accordingly and passes the data down the stack. Likewise, when the LLC receives a packet from the MAC layer it parses the *EtherType* field and passes the packet to the respective protocol [8].

The WSMP sends either WSAs (Figure 4), which announce availability of application services WSMs (Figure 5) that are generic data packets. A WSA can be sent secure or unsecured - in the latter case the 1609.2 Std specific fields are omitted. The WSM is composed of the LLC header, network header, transport header, and data. The network header indicates what networking subtypes are supported and the WSMP version. The transport header specifies the transport protocol by designating the address type to be used during transmission. Since the 1609.3 standard utilizes data structures specified in 1609.2 Security protocol, any malicious activity occurring within the security layer protocol could manifest within the network layers.

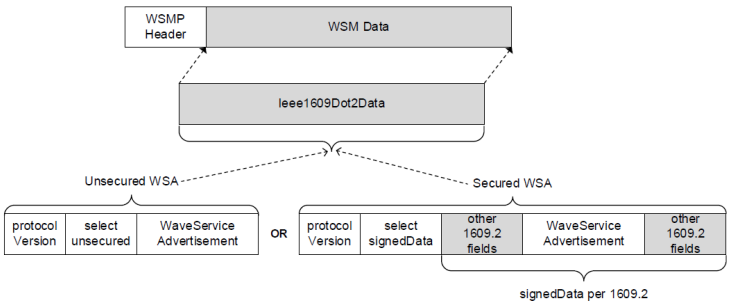

Figure 4. WAVE Service Advertisement Diagram.

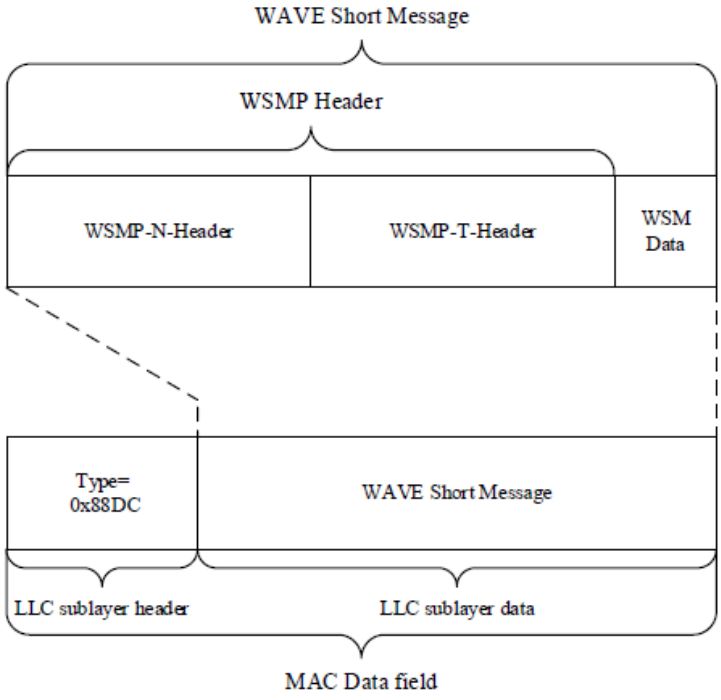

Figure 5. WAVE Short Message Diagram.

2.5 IEEE 1609.2 Security Services for Applications and Management Messages

IEEE 1609.2 Security Services provides the cryptographic operations that allow for secure communication between WAVE devices. It can be broken in two distinct halves:

1. **Internal Layer Security Services**
    - Security Data Services (SDSs)
    - Security Service Management Entity (SSME)
2. **Higher Layer Security Services**
    - Certificate Revocation List (CRL) Verification Entity

- Peer-to-Peer Certificate Distribution (P2PCD) Entity

The Internal Layer is comprised of SDSs and a security management entity. SDSs are fundamental in securing data transmission in WAVE. SDSs are invoked by Secure Data Exchange Entitys (SDEEs) when information is transmitted or received. When transmitting, the SDS converts data - called a protocol data unit (PDU) - into a secured protocol data unit (SPDU). A SPDU can be one of three types: unsecured, signed, or encrypted. When receiving, the process is reversed as the SDS receives a SPDU and converts it to a PDU. A SDS may be invoked several times because a SPDU may have multiple levels of encryption or decryption. Figure 6 depicts this exchange below. The second portion of the Internal Layer contains the SSME. The SSME retains all certificates and information pertaining to said certificates. When information is added to the SSME it is made available to all SDEEs who have access to the SSME.

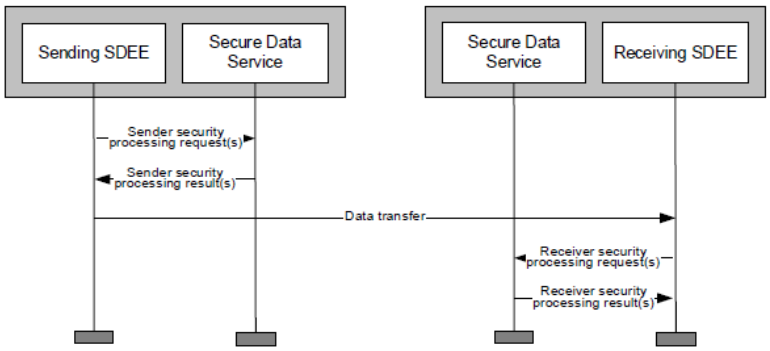

Figure 6. WAVE Service Advertisement Diagram.

The Higher Layer of the IEEE 1609.2 standard is comprised of two entities. The first, the CRL Verification Entity, validates CRLs as they are received. Once received, the CRL is sent to a SDS for verification. If verified, any relevant revocation information is passed to the SSME for storage. The P2PCD Entity is the primary component behind P2PCD functionality. P2PCD is triggered when a device receives

a signed SPDU and the issuer of the certificate is not recognized. The P2PCD entity will send P2PCD learning requests to peer devices in attempt gain insight on the unknown certificate [10].

2.5.1 Cryptographic Operations and Data Structures.

The data structure specified by IEEE 1609.2 for SPDUs is composed of three central types: unsecured data, signed data, and encrypted data which align with the three types of SPDUs. The SDS produces symmetrically encrypted data in one of two approaches: ephemerally or statically. The difference between the approaches is the first generates a new, random symmetric key while the second uses an established symmetric key for encryption. Asymmetric encryption is used to encrypt symmetric keys. Hashing is used in conjunction with the other cryptographic operations to confirm uniqueness of information. Certificates and signing is discussed in the next section. The cryptographic functions that are supported by IEEE 1609.2 are [10]:

1. Asymmetric Encryption: Elliptic Curve Integrate Encryption Scheme (ECIES)
2. Symmetric Encryption: Advanced Encryption Standard in Counter Mode with Cipher Block Chaining Message Authentication Code (AES-CCM)
3. Hashing: SHA-256
4. Signing: Elliptic Curve Digital Signature Algorithm (ECDSA)

Note: IEEE 1609.2 Security Services supports only the cryptographic algorithms listed above.

2.5.2 Certificates and Signing.

A certificate is used to transport cryptographic information between WAVE devices. This information includes: public keys, permissions, issuer identity, and re-

vocation data. The two notable types of certificates are explicit and implicit. An explicit certificate contains a public key whereas the implicit certificate contains a value used to derive the public key. A certificate chain is a group of certificates ordered in a linear fashion. As a certificate is added to the chain the issuing certificate is the adjacent certificate in the chain. The top of the chain is required to be an explicit certificate and is referred to as the trust anchor. When data is hashed for signing the data is given one of two verification values; *certificate* meaning the data will be verified with a certificate and *self-signed* meaning there is an identifier key within the data itself [10].

2.6 The Basic Safety Message

The BSM is the message format that is used by Vehicle-to-Anything (V2X) applications to transfer information to surrounding nodes. As the name suggests, safety is the primary function for the BSM. These messages are transferred at a rate of ten times each second. The BSM format is separated into two primary sections. The first is transmitted with every message and the second part is sent only when necessary such as emergency vehicle identity and safety event flags. Thus, the data contained in the second type of data is optional and not necessary for successful transmissions.

The BSM is defined by the SAE J2735 data dictionary and SAE J2945 requirements documents [11], [12], [13]. The breakdown of the message contents by type is shown below:

- **BSM Data Contents Part 1**

  This information is mandatory and sent with every BSM transmission.

  - Message Count: Provides a sequence number for messages that are sent from the same sender. Sequence numbers are limited from 0 to 127.

Senders can initialize this field to any value as senders may change their temporary ID's during a batch of messages.

- Temporary ID: Four octet random device identifier that rotates to protect device identity.
- Second: Represents the milliseconds within a minute. Expressed as an integer value from zero to 60999. A leap second is represented as values between 60000 and 60999. Values 61000 to 65534 are reserved. The value 65535 is used to signify an unavailable value.
- Latitude: The latitude of the object expressed in 1/10th integer microdegrees.
- Longitude: The longitude of the object expressed in 1/10th integer microdegrees.
- Elevation: The position of the object above or below the reference ellipsoid (WGS-84). The value has a resolution of 1 decimeter.
- Positional Accuracy: Used to model the accuracy of the position with respect to each axis.
- Transmission State: Current state of the vehicle transmission. Data element utilized is of type enum.
- Speed: Vehicle speed expressed in unsigned units of 0.02 meters per second. If unavailable, 8191 is used.
- Heading: Current vehicle heading expressed in unsigned units of 0.0125 degrees from North such that a value of 28799 degrees represents 359.9875 degrees. When data is unavailable, the value 28800 will be used. When stationary, the past heading value may be used.
- Steering Wheel Angle: The angle of the vehicle's steering wheel expressed

in signed values between -126 and 126 with each value represents LSB units of 1.5 degrees. A negative value indicates a left turn and positive values represent right turns.

  - Acceleration: Set of values containing three orthogonal directions along the longitude, latitude, vertical axis along with yaw.
  - Brake System Status: Contains all information related to standard brake and system control activity of the vehicle. Such controls as Traction Control System, Anti-Lock Brake System, Stability Control, etc.
  - Vehicle Size: Contains the vehicle length and width. Values are represented as centimeters and a value of zero will be utilized when unknown.

- **BSM Data Contents Part 2**

  The information contained in this section is broken into three data structures. This information is optional and only transmitted when necessary.

  - Vehicle Safety Extensions: This data is used by V2V safety applications to calculate event flags, path history, and path prediction.
  - Special Vehicle Extensions: This structure refers to vehicles that are excluded from normal traffic due to intent or ability. Examples are police vehicles, emergency responders, and alternatively, heavy trucks carrying hazardous materials. These vehicles are identified by additional certification permissions barring civilian usage of this field.
  - Supplemental Vehicle Extensions: This structure is used for additional V2V applications. It is a means to develop experimental message content.

2.7 V2V Applications

The safety benefits of V2V are made possible through multiple applications [14]. Through the use of the OBUs and RSUs, VANETs are dynamically created, joined, and exited by vehicles within a given area, and are used to exchange traffic related information. This allows drivers to take proactive actions when alerts are received for events such as high congestion, collisions, and similar events. Existing examples of V2V applications include:

- Emergency Electronic Brake Lights (EEBL)
- Intersection Motion Assist (IMA)
- Blind Spot Warning / Lane Change Warning (BSW/LCW)
- Forward Collision Warning (FCW)

These V2V applications are enabled through the exchange of BSMs between vehicles. Data such as speed, heading, acceleration, brake status, and steering wheel angle, are processed and alerts are displayed to the driver when potential threats are discovered. In the case of Intersection Motion Assist, an alert is issued when one of two cars determine that there is a collision imminent. Once delivered, the drivers retain responsibility to prevent the collision from occurring (slow down, swerve, etc.). For these applications to be possible, both vehicles need to be equipped with V2V equipment.

When these V2V applications are coupled together, high level management protocols are possible. One protocol, platooning, is where vehicles with similar routes group together. This allows vehicles to maintain speed and heading for longer periods of time. Platooning also incorporates physical sensors attached to each vehicle which allows for each vehicle to monitor the distance of other vehicles in their immediate

vicinity. These sensors, typically radar-based or light-based, have been installed on production vehicles since the mid-1990s and are referred to as Adaptive Cruise Control (ACC). This allows vehicles to alter their speed based on vehicles traveling in front of them - without input from the driver. V2V combined with ACC is known as Cooperative Adaptive Cruise Control (CACC) and is what allows platooning to function. The benefits of platooning allow for improved traffic throughput as vehicle density increases (more vehicles can be packed closer together) without increasing commute times. In addition, fuel consumption is improved as vehicles are able to draft behind lead vehicles.

2.8 Security Exploits

The most important requirement of implementing V2V communications is security. Developers must consider each aspect of the security triad (Confidentiality, Integrity, and Availability) to allow vehicles to communicate sensitive information without fear of malicious activity. Poor security implementation of V2V can have a direct impact on human life. This section will review three distinct security attack vectors in V2V, the effects of each, and what methods researchers have proposed to mitigate said vectors.

2.8.1 Sybil Attack.

A Sybil attack is a scenario where a malicious node replicates multiple fake nodes. The fake nodes would be able to spoof messages to actual nodes over saturating the network. If successful, the malicious node has the ability to control the network. Sybil attacks were first described in peer-to-peer scenarios [15]. It is possible for this attack to extend to VANETs.

In [16], the authors describe a solution where each RSU determines three pa-

rameters for each unique beacon packet it receives from a vehicle and uses them to determine legitimate users from false users. These parameters include Received Signal Strength, distance of vehicle to RSU, and the angle from vehicle to RSU. Over time, this allows RSUs to accumulate data and determine if nodes are moving at the same distance and vector suggesting the nodes are Sybil nodes and can be blacklisted. According to their findings, this technique displays high levels of accuracy identifying Sybil nodes with a low false positive rate. However, there are two distinct hurdles that this technique generates. Firstly, relying on RSUs to compute these three parameters for each vehicle in the VANET can become computationally expensive quickly. Processing can be lessened by increasing the amount of RSUs but this is not a logistically feasible solution. The second obstacle is the lack of RSUs in rural areas. Low density population areas have few incentives for RSU placement. This creates dead zones where Sybil attacks have a higher chance of succeeding. This drawback could be a accepted risk considering there is little reward for malicious attackers to deploy such attacks in rural areas.

2.8.2 Denial of Service / Jamming.

A Denial of Service (DoS) attack occurs when an attacker floods a network with an abundance of useless messages at a rate faster than the users on the network can possibly process. Jamming is similar to a DoS attack as the attacker creates interference on the network which disrupts the transfer of legitimate messages from sender to receiver. With respect to WAVE, DoS or jamming attacks can occur on the CCH when safety critical WSMs are sent [17].

The effects of these kinds of attacks are fortunately hindered by the fact that loss of V2V communication does not impede functional capability of the vehicle under attack. The only effect is that a driver will not be able to send or receive safety

messages from surrounding V2V-equipped vehicles and RSUs. The potential issue arises is when vehicles are in a platoon [18]. Thus, in scenarios where V2V determines vehicle movements jamming could potentially lead to a collision.

The mitigation of this attack is built into the security layer IEEE 1609.2 - the CRL. The CRL contains revocation information pertaining to certificates that have been deemed untrustworthy. In this case, if an attacker has been found committing a DoS attack, their certificate identity is added to the CRL by the CA. The CA disseminates the revised CRL to RSUs which then disseminate to each passing vehicle and those vehicles disseminate to any vehicle that has not yet received the revised CRL from a RSU. The drawback to this solution is in locations with low RSU density it can take a large amount of time before a vehicle can receive a revised CRL [19].

2.9 Certificate Requirement

NHTSA has proposed the use of PKI digital signatures for BSM verification. This process involves every message to be signed by the sending device along with a valid certificate. The certificate is composed of the date range that depicts the validity of the certificate, the public key corresponding to a private key, and the digital signature from a certificate authority. When a device receives a BSM it looks at the certificate to verify that the signature is from a valid CA, and if so, the contents of the message can be trusted. The receiving device does this by comparing the signature to an already stored signature from the same CA. If the device does not have the signature, the device sends a request to the CA of the sending device. The creation and verification of a signed BSM is listed below.

Signed BSM Creation

1. Compute the hash of the message content using SHA-256.

2. Generate a digital signature by inputting the hash contents by using ECDSA.

Verifying Signed BSM

1. Generate the hash of the message contents using SHA-256.

2. Verify signature by using the hash, public key, and signature though ECDSA.

3. Verify the digital signature back to the root certificate.

4. Verify the pseudonym certificate is not on the CRL

These two processes are depicted below in Figure 7.

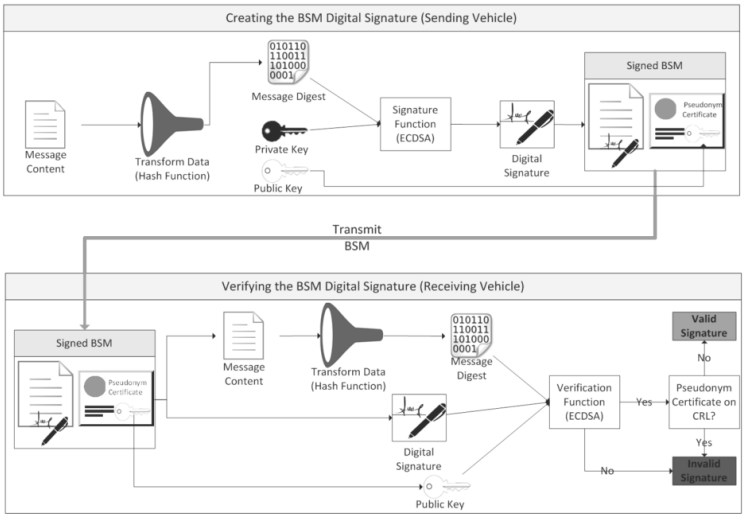

Figure 7. The creation and verification of a signed BSM [1]

PKI allows for trusted and verifiable messages to be sent over public networks. In typical public networks, sending and receiving entities are mutually known and verified. When organizations need to make private interactions they rely on pre-existing agreements with the CAs . However, in VANETs, this process is increasingly more complex as consumer location privacy is introduced. Vehicles are expected to verify digital signatures without identifying the sender in order to retain privacy. Any single entity that has the ability to record location history would decrease public acceptance of V2V whether that entity be a CA, law enforcement, or malicious actors.

In addition, the large number of users proposed is unparalleled to any equivalent network. Thus, an entirely new system is required to define the security infrastructure that applies to the needs of V2V communication. NHTSA has chosen the SCMS framework as the leading candidate design [20].

2.9.1 Security Credential Management System.

In [20], SCMS is set apart from other PKI implementation by allowing for high volume of users as well as a balance between security, privacy, and efficiency. In the US, full capacity is assumed to be three hundred million vehicles. With nearly one thousand certificates per vehicle per year the SCMS is expected to undertake issuing and managing three hundred billion certificates. To preserve privacy, responsibilities are distributed to multiple authorities to prevent any one entity to obtain complete identifiable information of any vehicle yet still perform necessary security functions in an efficient manner. The individual components of the SCMS are listed and described below. These components are depicted in Figure 8 below.

- Root CA: Provides the self-signed root certificate that provides the basis of the PKI implementation.
- Intermediate CA: Can be used as proxy root certificates.
- SCMS Manager: Overseas operation of entire SCMS, most notably setting the principles for misbehavior and revocation requests.
- Certification Services: Specifies the certification process that determines which devices are to receive digital certificates.
- CRL Store: Receives CRL from the CRL Generator. Its main purpose is to maintain and share CRLs

- Enrollment CA: Issues enrollment certificates which allow a device to request pseudonym certificates.
- Device Configuration Manager: Provides authenticated information about SCMS to devices
- Device: A OBU or RSU that transmits BSMs
- Linkage Authority: Generates linking values which are utilized inside certificates. The SCMS design specifies two linkage authorities which prevents linkage operators linking certificates to a specific device
- Location Obscurer Proxy: Prevents location detection by masking source addresses. When reporting to the Misbehavior Authority, it shuffles the reports to prevent the MA from determining routes.
- Misbehavior Authority: Processes misbehavior reports and, if necessary, adds misbehaving devices's certificates to the CRL. The MA contains three sub entities which are: Internal Blacklist Manager which keeps information on components of the SCMS that may be misbehaving, Global Detection which determines which devices are misbehaving, and CRL Generator which issues the CRL for distribution.
- Pseudonym CA: Issues the short-term certificates to devices.
- Registration Authority: Receives and transfers pseudonym requests to the Pseudonym CA.
- Request Coordination: Checks that a device does not request multiple sets of certificates for the same time period.

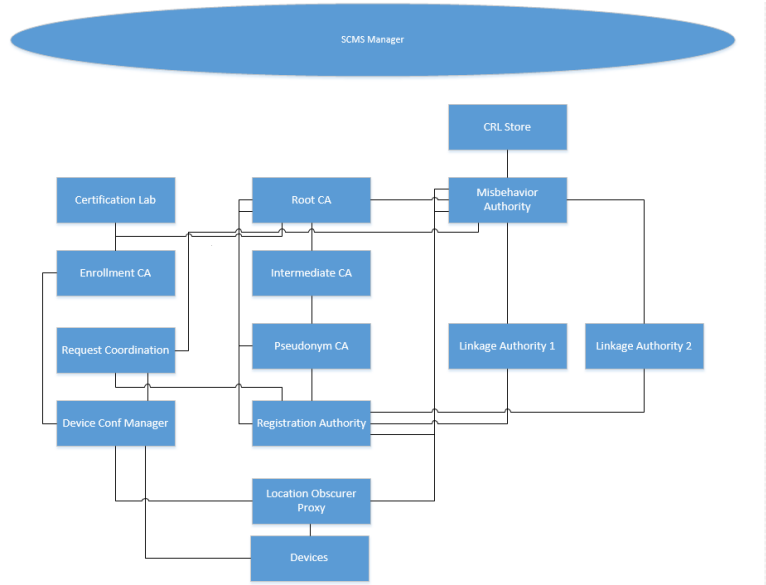

Figure 8. SCMS Design Overview [21]

In order to preserve privacy, certain components of the SCMS are separated to prevent any one entity from acquiring enough information to determine device identity. The pseudonym CA and registration authority must be two separate entities otherwise a single entity would be able to identify which pseudonym certificates have been issued to devices. In addition, the pseudonym CA and linking authorities must be two separate entities as the pseudonym CA would be able to link pseudonym certificates from the global pool to a device since the linking authorities know the linkage values that make a portion of the certificate and the pseudonym CA sees these values at the time of certificate generation. There must be multiple linking authorities to prevent a single authority to link certificates. The Location Obscurer Proxy is its own entity otherwise components would be able to determine location of vehicles. The SCMS Manager should independent as it sets policies and is not necessary for regular operation. If not, the SCMS Manager could obtain global knowledge potentially leading to privacy loss. The Misbehavior Entity should be its own entity otherwise it could bypass SCMS policies. Lastly, the root certificate should be independent and

ran by a trusted organization.

2.9.2 Vehicle Based Security System.

NHTSA has also investigated an alternative certificate management design to that of the SCMS. Like stated above, a device in the SCMS communicates with the pseudonym CA to request pseudonym certificates. Under the VBSS, a device assumes the role of the pseudonym CA reducing the necessity of a pseudonym CA and all entities associated with it. In the end, the pseudonym CA, registration authority, linking authorities, and request coordination entities are all removed. The system creates Group Managers that provide credentials for each device to become their own authority.

In VBSS, a device is attached to a group and is given a unique secret signing key. All keys within a group are established with a single group certificate. A device creates its own pseudonym certificates by signing the public key with its group key and thus devices are subordinate CAs and pseudonyms are generated when needed. Verification is completed by using the group certificate to authenticate the pseudonym certificate, and then the pseudonym certificate to verify safety messages. Message exchanges are anonymous since the receiver only sees the group certificate and not a specific device's certificate. Groups are managed by RSUs and can update group membership validity by updating the group certificate and providing it to those that need to stay within the group. By using pseudonyms and separating distributed identifiers VBSS claims it achieves an acceptable level of privacy. However, VBSS remains the alternative choice as group-based certificate schemes are not as mature as other forms of cryptography. Figure 9 below shows the VBSS component interaction. Table 1 below compares the entity differences between the SCMS design and VBSS design [22].

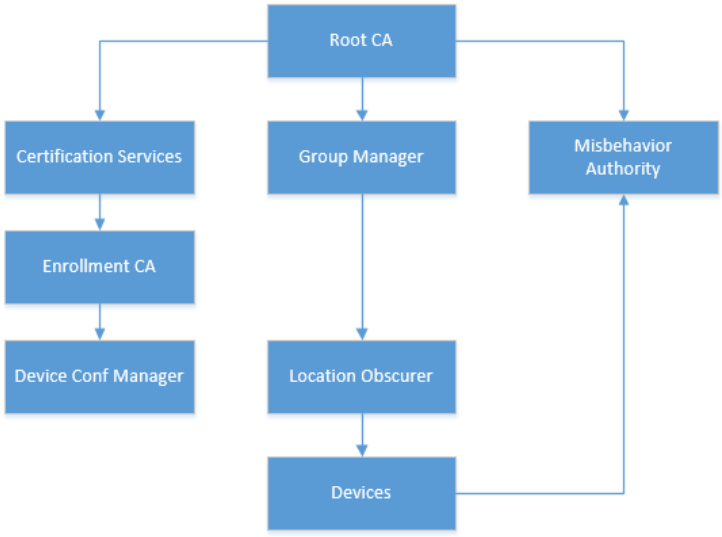

Figure 9. Vehicle Based Security Services Diagram [1]

Table 1. Comparison Of SCMS and VBSS Components

Common Components	SCMS	VBSS
Root CA	Linkage Authority 1-2	Group Manager
Certificate Services	Pseudonym CA	–
Device Configuration Manager	Registration Authority	–
Location Obscurer Proxy	Request Coordination	–
Misbehavior Authority	SCMS Manager	–
Enrollment CA	CRL Store	–

Whether the SCMS, VBSS, or a variation of both is adopted the security management behind V2V communication will be elaborate and certainly unlike any other established cryptographic system. Aside from the root CAs and intermediate CAs almost every entity described within the SCMS is novel which will require intensive testing and multiple iterations of proofs-of-concept. Certificate revocation is a complex aspect for both schemes. CRLs within traditional unique pseudonyms (i.e. SCMS) are hindered by list growth, revocation determination, and efficient look up times [22]. In VBSS, a single misbehaving vehicle causes the revocation of an entire

group certificate. Alternate certificates could alleviate this issue but this would also increase complexity and size - aspects that VBSS strives to improve upon from SCMS. The following section will discuss past research and mitigation of certificate linking.

2.10 Related Work

This section will give an overview of NHTSAs Notion for Proposed Rulemaking which is an aggregation of V2V design components, timeline, and manufacturer comments. In addition to this document, research conducted by MITRE on behalf of NHTSA is presented in regards to pseudonym linking and proposed mitigations to pseudonym linking. Lastly, the three data flows described within NHTSAs Privacy Impact Assessment are discussed as well as comments from the academic community on NHTSAs proposed rulemaking.

2.10.1 National Highway Traffic Safety Administration.

In early 2017, NHTSA released a Notice of Proposed Rulemaking (NPRM). The extensive document was the result of many years of research and development of the V2V standard. The goal of this document was to propose a federal mandate for all new light passenger vehicles to be equipped with V2V communication. The agency firmly believes that by introducing V2V communication, vehicle crashes will be able to be reduced therefore lessening loss of life and destruction of resources [1].

The NPRM states that V2V communication is superior to current "vehicle-resident" crash prevention technology such as cameras and sensors. This is because V2V has the capability to detect other V2V-capable vehicles around blind corners and through other vehicles. Current vehicle-resident technology such as cameras and similar sensors are limited by line-of-sight. V2V also increases path prediction of other vehicles as information such as steering angle and brake status are transmitted within the

BSM. This allows for drivers to more accurately perceive the intended actions of other drivers - especially useful within intersections. V2V communication is capable of transmitting three hundred meters, almost double the range of many vehicle-resident sensors allowing for potential hazards to be detected farther in advance than sensor-based alerts. V2V communication is not subject to the elements where sensors can be affected by rain, light, and dirt.

However, NHTSA points out that V2V communication is not a replacement for current sensor-based driver alert systems. On the contrary, V2V would complement sensors-based alerts as they can detect non-V2V equipped objects in direct vicinity of the vehicle. For example, lane and road departure warnings in addition to wildlife that may dart across the road at a moments notice. V2V communication and vehicle-resident sensors will be able to act as a checks and balances system where one system will verify the findings of the other system. For example, in the event of a Sybil attack, a vehicle would be able to utilize sensors to validate incoming V2V messages. While these capabilities are relatively short term, NHTSA believes long term capability of the mesh of these two technologies will further the development of automated vehicles even to the point of true fully autonomous vehicles.

Despite the benefits listed above they do not come about without hurdles. For V2V communication to become widespread, three major stakeholding parties must be persuaded that it is beneficial to vehicle safety. These three parties are: the legislative bodies, the automobile industry, and consumers. For consumers to adopt V2V communication they must, among other things, trust that the technology will not unduly infringe on their privacy. This hurdle is particularly difficult in today's political climate where hacking is widespread and prevalent. Legislators also need to be persuaded that V2V is beneficial to the consumer and will not decrease privacy. Finally, another stakeholding party to consider is automobile manufacturers

as they are the ones who must integrate V2V into their current platforms. This is more easily done with the other stakeholders since manufactures are accustomed to designing vehicles around several government mandates such as airbags, seat belts, and similar safety requirements. V2V does not impose any physical limitations other than OBU installation so it is fair to say that integration of V2V communication will not significantly hinder manufacturer vehicle designs.

2.10.2 Proposed NHTSA Certificate Changing Method.

With NHTSA pushing for a mandate to require V2V on all new vehicles there are several areas that remain dubious. One such research areas is the notion of changing certificates. Using data learned from the Safety Pilot: Model Deployment program NHTSA researchers developed a revolving certificate design where a vehicle utilizes a single certificate out of a pool of twenty [23]. After five minutes the vehicle alternates to another certificate from the pool. This process continues for a week when the pool is discarded and a new pool is utilized. NHTSA believes that design allows for both consumer privacy as well as efficient management of certificates.

2.10.3 Misbehavior Detection.

Proper misbehavior detection is critical for V2V devices to establish a foundation of trust between one another. This is to include devices to self-diagnose themselves (similar how vehicles have Check Engine Lights, etc.). Misbehavior detection provides a method for V2V devices to identify "bad actors" and determine whether messages from these individuals should be ignored or blocked. If an incident has been detected, information from the transgressor will be accumulated by the reporting device and transmitted to proper authorities. NHTSA believes that a misbehavior authority shall be incorporated to review such reports for authenticity. If determined authentic, the

misbehavior authority will pass the misbehaving device's certificate to the SCMS who places it on the CRL. Without misbehavior detection in place, trust between vehicles would degrade as misbehavior would go unchecked. In addition, misbehavior reporting will need to be handled properly to prevent wrongdoers from obtaining a simple attack vector.

However, NHTSA admits that additional research is required to better understand data, processing, and algorithm development necessary to introduce a misbehavior detection scheme into V2V communications. NHTSA has requested comments regarding misbehavior detection requirements, detection and identification techniques, and identification capabilities over time. To do so with meaningful contributions, misbehavior needs to be adequately defined such that identification techniques can be developed and applied. For purposes of this work misbehavior will defined in the following ways:

- Non-moving Misbehavior: Types of behavior that are included in this category are misbehaviors that refer to a vehicle's OBU, surrounding OBUs, and surrounding RSUs. Any device that is not performing at specified BSM operating requirements, either by malice or by malfunction shall be within this category. These operating requirements are defined in SAE J2945. NHTSA proposes the following types of misbehavior suspicion types:
  - False Warning Report
  - Proximity Plausibility
  - Motion Validation
  - Content and Message Verification
  - Denial-of-Service Detection
- Moving Misbehavior: This category is refers to any V2V vehicle in motion that

performs an act of misbehavior. It should be noted this does not refer to a misbehaving V2V device but rather the misbehavior of the vehicles and therefore the drivers themselves. This definition goes beyond the notion of misbehavior that NHTSA presents yet should be accounted for, as the possibility for V2V to detect such misbehavior is present. This type of misbehavior can be described in two categories: unethical and illegal. Unethical misbehavior describes vehicles that do not follow established practices such as right-of-way rules, cutting off other vehicles, and others. Illegal misbehavior describes not following established traffic laws such as red-light running, hit-and-run collisions, and others.

2.10.4 Misbehavior Reporting.

After misbehavior has been detected, a report shall be generated with sufficient information to determine if misbehavior has occurred. Due to the sensitive information being stored persistently NHTSA has stated that any misbehavior reports must be encrypted. NHTSA has suggested the following information to be included:

- Reporter's pseudonym and certificate
- Time and Location
- Devices within range
- Speed
- Suspicion type(s)

2.10.5 Privacy Implications.

With the introduction of V2V communication, vehicle and driver privacy is at risk. How does V2V - a system designed to disclose vehicle data - also prevent the disclosure of data that impedes on consumer privacy? These two concepts inherently contradict

each other. Public opinion is one of the biggest hurdles V2V has to overcome for adoption and it is unlikely consumers would adopt technology that could potentially create location tracking capabilities. NHTSA has spent considerable time and effort on this topic. To address this issue, NHTSA released a Privacy Impact Assessment that addresses these tracking concerns [3]. This document breaks down three flows of data that hold potential for tracking to occur.

- BSM Broadcasting and Receiving - The first is the sending and receiving of BSMs between vehicles. As discussed earlier, BSMs provide the fundamental functionality for V2V application such Forward Collision Warning (FCW), Emergency Electronic Brake Light (EEBL), and Intersection Motion Assist (IMA). The information that these messages contain may be harmless when observed at discrete times and singularly, but aggregated over the course of time may lead to identifying patterns compromising privacy. BSMs are not encrypted which opens up the possibility of third-party observers collecting these messages; for good or malicious activities. V2V devices (OBUs, RSUs) are not authorized to store BSMs for longer than what is necessary for safety or malfunction purposes.

- Misbehavior Broadcasting and Receiving - When a V2V device receives a BSM the contents are cross checked to validate the credibility. This may be done using other vehicle-resident sensors or from other BSMs from neighboring devices. Messages that do not pass this "fact check" are identified and a report is generated by the reporting device and sent a subset of the SCMS. The SCMS evaluates this misbehavior report and if the SCMS determines that the report is valid it will add the certificate associated with erroneous messages to the CRL. This blacklist tells all others V2V devices to use caution when receiving the revoked certificate. Misbehavior reports include the reporting BSM, transgress-

ing BSM, as well as any alerts that were issued by surrounding devices that could support or refute the misbehavior that is suspected. With respect to privacy, misbehavior reports are retained for longer periods than typical BSMs and include BSMs from neighboring vehicles that may not want their information contained within the report.

- Certificate Revocation List Distribution - The last flow of data NHTSA discusses as a potential avenue for data leakage is the distribution of the CRL. The security manager places certificate identifiers on the CRL that are appropriately deemed to be misbehaving. These identifiers are a time stamp, linking seeds, and associated linking authorities. OBU would be able to compute the certificates from these values.

In order to prevent data leakage from these avenues NHTSA, along with industry partners, has pushed a "privacy by design" approach for the SCMS. Accounting for privacy and security from the initial design allows for a more secure deliverable. NHTSA released decrees that propose to increase privacy with respect to the three data flows listed above. The primary control - directly identifying or "reasonably linkable" data is not permitted to be exchanged - has received scrutiny from experts within the security community [24]. The Center for Democracy and Technology (CDT) states that data within BSMs are relatively simple to link and no mitigation controls proposed by NHTSA are sufficient. Below are the aspects that the CDT describes that lack privacy mitigation controls.

- Individual Linking - NHTSA has proposed the notion that BSMs shall transmit location with accuracy up to 1.5 meters. The CDT states that this high of accuracy would compromise specific vehicle location during times that would be unnecessary such as in parking lots, driveways, and other low speed or non

moving events. This could contribute to identification of vehicle ownership and vehicle residence. They conclude by pointing out that this leads to driver identification since shift workers, 9:00 a.m. to 5:00 p.m. workers, students, and stay-at-home parents all have different identifiable driving patterns.

- Linking Certificate Changes - The CDT references the current certificate switching method by indicating five-minute lifetimes makes it simple to link BSM during this interval. Additionally, even after certificate changes, linking BSMs with two different certificates is only slightly more challenging. Using the contents of the message, certificates could be linked. They give the example that a vehicle traveling at 60 mph moves only 2.7 meters in between BSM which is lower than the typical distance between successive vehicles allowing for BSM linking.

- Linking Message Content - The CDT points out that information in the message can be linked to vehicle and therefore individuals. BSMs include vehicle size within an accuracy of 0.2 meters. The CDT categorized 343 vehicles and determined that the 0.2 meter accuracy resulted in thirty categories of vehicles. Out of thirty categories, seven included only one vehicle and eight only included two vehicles. The example is given that a F-250 and Ram 3500 share a category with no other vehicle. Two BSMs sent with a reasonable amount of time in between can be linked to a single vehicle with high confidence regardless of certificate changeover. Vehicles with identical dimensions will differ through other attributes such as speed, acceleration, steering angle, and yaw as these all differ between make and model. This will allow for vehicle identification.

- Linking Certificates - The CDT states that the proposed certificate changing method allows for an eavesdropper to listen to a vehicles certificates and gather a significant portion of them just using a single location the vehicle frequents

(e.g. driveway, workplace, etc.). They speculate that if a vehicle is driven for one hour a day then eighty four certificate changeovers occur every week. An eavesdropper could, again, listen to these changeovers and link weekly changeovers.

- Associative Linking - If an eavesdropper is receiving BSMs from three vehicles traveling along the same route with near identical speeds and it receives a certificate changeover then it deduces using the techniques above which certificates to associate with respective BSMs.

- Transmission Range - NHTSA has stated that the minimum range for the range of a BSM is three hundred meters but does not set maximum range or power to limit the transmission radius. The CDT mentions that limiting transmission range does not prohibit observers to use sophisticated antennas to listen in on V2V broadcasts.

- V2V Tracking vs. Non-V2V Tracking - NHTSA compares V2V tracking to other forms of vehicle tracking to point out that would be the path of least resistance to a malicious actor. The non-V2V based tracking methods they identify are physical surveillance, planting GPS device on a vehicle, physical access to vehicle-resident GPS logs, electronic toll transactions, cell phone history, On-Star and similar devices, traffic cameras, and license plate transcribers. The CDT points out that while these are all possible, but there is one critical difference. V2V-based tracking allows for mass-surveillance while the non-V2V tracking techniques are specific to a single vehicle. The example they give is a malicious actor with one well-placed V2V receiver can monitor an entire neighborhood with relative ease.

- Privacy Statement Inadequacy - NHTSA has proposed a privacy statement that will be supplied with all V2V vehicles purchased. The CDT argues that

the statement in its current form is misleading to consumers. The statement utilizes the verbiage "data that is not reasonably or, as a practical manner, linkable to you". This statement is intentionally left open to interpretation; for better or worse. The privacy statement also includes how third parties are allowed to listen to BSM traffic and only mentions the beneficial reasons for this (e.g. accident avoidance, reduced congestion), but do not mention how third party collection could be used for nefarious purposes.

2.10.6 Modeling and Simulation of Areas of Potential V2V Privacy Risk.

In March 2016, MITRE released a technical memorandum entitled "Modeling and Simulation of Areas of Potential V2V Privacy Risk" [25]. The purpose of this work was to study the privacy impacts by the broadcasts of BSM from OBUs and RSUs from within a VANET environment. MITRE utilized the traffic modeling software Simulation for Urban Mobility (SUMO) to generate datasets to fulfill this objective. MITRE made the determination that the frequency of certificate changing and the capability and capacity to collect BSMs is directly related the ability to track a V2V device. Untargeted tracking and targeted tracking were both investigated for this study. Untargeted tracking consisted of two geographical scenarios collecting all BSMs possible. Targeted tracking consisted of choosing a single V2V vehicle. The two principal variables MITRE uses in this study is RSU density and certificate lifetime rate. RSU density was measured between 25% to 100% in 25% increments (percentage indicates the amount of BSMs received by RSUs). Certificate lifetime rates were varied between one and five minutes (in one minute increments).

In the two different geographical scenarios for untargeted tracking, MITRE determined that shorter certificate lifetimes coupled with lower RSU density reduced the

possibility of tracking significantly. In addition to the primary variables, MITRE also considered vehicle size and path history; two data points that are transmitted within the BSM. In instances where a vehicle could not be matched to a previous certificate, MITRE was able to use path history or vehicle size to match vehicles. Targeted tracking was divided into two categories - static RSU based tracking and mobile based tracking. Both instances require prior identification. RSU-based targeted tracking achevied comparable results to that of untargeted tracking. Mobile tracking was simulated by having a vehicle follow a victim vehicle and capture its BSMs as well as any other BSMs that were received along the way. The trailing vehicle was able to track the vehicle as long as the two vehicles remained within three hundred meters of each other. If the separation exceeded three hundred meters, then the trailing vehicle would only be able to restore positive identification if the separation dropped back below three hundred meters before the vehicle's certificate was rotated.

MITRE concluded that untargeted tracking is possible given the computational resources to analyze the data. Due to the high computational overhead, large-scale vehicle location tracking in real-time would be unlikely do to the level of difficulty. However, when targeting a specific vehicle, real-time tracking is possible due to the low overall computation needed. MITRE addresses the fact that successful V2V tracking hinges on access to systems, ability to analyze accumulated data, and the level of coordination necessary to aggregate BSMs.

2.10.7 Certificate Linking Mitigations.

Referring back to the SCMS and VBSS much of the design characteristics are chosen to deter privacy leakage of individual devices from occurring. Perserving consumer privacy is critical to public acceptance of V2V communication. This section reviews three privacy preserving techniques specialized for the VANET environment.

2.10.7.1 Silent Period.

In [26], the first mitigation discussed is the utilization of a silent transmission period to thwart the linking of pseudonym certificates. A device will cease transmitting messages at random times decreasing the chance of eavesdroppers linking sequential transmissions. However, as pointed out in [27] this technique can be defeated by Bayesian traffic analysis. This technique utilizes the messages sent before and after the silent period to link messages. In addition, ceasing safety transmissions would hinder the functional purpose of V2V and would be limited to short periods further increasing odds of linking.

2.10.7.2 Group-Based Pseudonyms.

The second mitigation discussed in [26] is the use of spatial group-based pseudonyms. Vehicles traveling in the same vicinity typically share redundant information (e.g. heading, speed, traffic observations). Because of this, in many V2V applications, every vehicle would not need to send information since many messages would be identical or nearly identical. In addition, vehicles are restricted in a number of ways: geographically by the roads they travel, velocity by speed limits, and direction due to the nature of road lanes. It should be noted that edge cases exist that are the exception to these observations. Vehicles could veer off the road, increase speed, and change direction in short amounts of time.

After these observations are made, vehicles traveling together could form groups. Since these vehicles are traveling together only one vehicle from the group would need to send messages on behalf of the group. The other vehicles within the group could remain silent during this time. This allows for a reduction in redundant information being transmitted as well as a reduction in pseudonym certificates since vehicle traveling silently would not need to rotate pseudonyms as frequently. However, the authors

observe that safety implication could arise through the use of the group pseudonyms.

2.10.7.3 RSU Coverage Restriction.

The last mitigation [26] discusses is limiting RSU placement. By establishing RSU coverage gaps vehicle location tracking could be decreased. By doing so, overheard and non-overheard regions are created. Overheard regions are when a vehicle can be heard by an RSU and non-overheard regions are when a device can not be heard by an RSU. The idea is for vehicles to rotate pseudonyms when in non-overheard regions. However, this concept would be susceptible to the Bayesian analysis where eavesdroppers would correlate the time a vehicle left an overheard zone with its speed and the time a vehicle entered the next overheard zone. In addition, NHTSA permits third-party listening meaning a third-party organization could install third-party receivers with 100% coverage.

2.10.8 Automatic Dependent Surveillance-Broadcast.

Many of the same security concerns that plaque V2V communication carry over to the aviation realm of Automatic Dependent Surveillance–Broadcast (ADSB). Similar to what NHTSA is proposing for V2V, the Federal Aviation Administration (FAA) has mandated all aircraft to be equipped with ADSB Out by January 1, 2020 [28]. ADSB allows for aircraft to broadcast information such as position, speed, and other data. By doing so, pilots would benefit from the safety alerts similar to that of V2V. However, message interception and spoofing are threat avenues because encryption and authentication mechanisms are not implemented [29]. The decision for this was made based off the trade-off of safety and privacy. The FAA was determined that safety was the utmost purpose of ADSB and the drawbacks from communicating unencrypted and unauthenticated were accepted risks. After all, majority of individ-

uals do not own personal aircraft and flight itinerary are already publicly available. Switching lanes back to V2V, could this decision uphold in the larger environment of VANETs?

2.11 Privacy Law

In [30], the author illustrates that privacy problems are hastily boiled-down to the response of "That violates my privacy!" and often lack sound argument of why the privacy problems are harmful. The lack of understanding of what privacy means and how it will be protected results in headaches for policy makers as the definition of privacy seems to transform from one scenario to the next. The author states that the problem is that the term "privacy" blankets many things that, while related, cannot be condensed into one single term.

In attempt to better define privacy this author depicts a taxonomy of four actions that impede one's privacy. These categories are further broken down into subcategories. These subcategories will be discussed in a case-by-case basis with respect to their relevance within the realm of V2V.

2.11.1 Privacy Law Taxonomy.

The following subcategories constitute the privacy law taxonomy.

- Information Collection
- Information Processing
- Information Dissemination
- Invasion

These four categories are sequential in order of how an entity would, if successful, impede a person's privacy. The first category is Information Collection. This

category is divided into two subcategories: Surveillance and Interrogation. With respect to V2V, surveillance will only be discussed as interrogation is not relevant to the VANET concept. The author depicts surveillance as the watching, listening, and recording of an individual's activities. This directly correlates with the V2V third-party collection of vehicles' BSMs. The author gives the example of *United States v. Knotts* where police installed a tracking device on the defendant's vehicle. The Court ruled that "amounted principally to the following of an automobile on public streets and highways." and stated that the Fourth Amendment did not apply because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." However, this case only considered the scenario of tracking a single vehicle. Third-party V2V message collection would enable mass surveillance of every V2V vehicle.

The author defines Information Processing as the way collected information is utilized by the collector. Information processing is further categorized into Aggregation, Identification, Insecurity, Secondary Use, and Exclusion. In terms of V2V communication, aggregation would occur after collecting BSMs and associating the same BSMs with the vehicle that transmitted them. Insecurity is the result of mishandling of collected information. The V2V analogy for Insecurity would be if a third-party organization allowed for release of collected BSMs through inadequate database protections. Secondary Use refers to the use of data for reasons unrelated to the initial purpose of the data. V2V data collection or usage is not regulated therefore the number of use cases for V2V data is open-ended. It is hoped that this information will be utilized for good such as traffic mobility and maintenance and not for nefarious reasons such as tracking and stalking individual vehicles, and by extension, individuals themselves. The last subcategory of Information Processing is Exclusion. The author points out that among the Fair Information Practices there are three central prin-

ciples: the existence of record keeping systems cannot be kept secret; an individual must be able to determine how information is used and stored about them; and an individual must be able to correct information about them. Failure to complete these principles would be Exclusion. The author describes that Exclusion, like Insecurity and Secondary Use, leads to feelings of powerlessness and vulnerability. In the event of a V2V mandate, consumers would have no choice but to disclose information which may lead to such feelings.

Information Dissemination is the broadest category as it covers the consequence of openly available information - a topic that strikes the core purpose of V2V communication. The author breaks down Information Dissemination into seven categories: Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, and Distortion. The first - breach of confidentiality - relates to public disclosure of information. With regards to unregulated third party collection the "third party doctrine" could possibly apply for such situations. The doctrine states that if information is possessed by third parties then the individual relinquishes a certain expectation of privacy per the Fourth Amendment. The author states that this is based on the secrecy paradigm - if secret information is known by two parties then the information is not secret. The example for V2V would be the dissemination of V2V information without permission or knowledge of the V2V users. Disclosure is similar to breach of confidentiality, however, the difference is where the harm is attributed. In breach of confidentiality the harm is dissolving of trust between two entities. In Disclosure, the harm is to the individual that the disseminated information was about. Simply put, disclosure is the allowing of information to spread outside its reasonable boundaries. A simple V2V scenario would be a third party disclosing locations of last known vehicle transmissions. Typically, these locations would be living or working locations. If a malicious actor gained this information they could

use it for nefarious purposes. Next, Exposure, would be release of information that would embarrass or degrade an individual. Thus, is it included with disclosure.

Increased Accessibility refers to how readily available information is to outside sources. The author depicts that with increased accessibility, the difference of quantity becomes a difference in quality. The author relates this issue to aggregation as it was recognized in *United States Department of Justice v. Reporters Committee for Freedom of the Press* that researching through public record, archives, and other decentralized forms of information is separate from a fully assembled dossier. Without V2V, it is relatively simple to track an individual vehicle either by physically tailing or installing a GPS tracker. However, mass surveillance with this technique of vehicles is near impossible. Now, with the introduction of V2V, mass surveillance can be obtained with V2V receivers. Third-party collectors only need to obtain V2V receivers in order to gain access to V2V messages.

Blackmail, or extortion, is the use of dissemination of information as power over an individual. In the case of V2V, the definitions for disclosure should suffice. Appropriation is the use of information to commercialize an aspect of an individual. This subcategory does not fit within the realm of V2V and will be not discussed further. Lastly, Distortion is damaging an individuals reputation typically through inaccurate statements. With respect of V2V, an example could be if a third-party released modified location records of an individual in attempt to tarnish that individuals reputation. For individual's seeking public office, such actions could prove detrimental to their career.

The last category the taxonomy presents is Invasion. This category is separated into two subcategories: intrusion and decisional interference. Firstly, Intrusion involves invasions or incursions into one's life. The author states "It disturbs the victims daily activities, alters his/her routines, destroys his/her solitude, and often

makes his/her feel uncomfortable and uneasy". Intrusion can be related back to Information Collection as surveillance and interrogation can lead to feelings listed previously. The harm of intrusion differs where feelings of paranoia - justified or not - lead to changes in one's daily activities. V2V surveillance could undoubtedly lead to such beliefs and actions. Lastly, decisional interference refers to the unwanted incursion by the government into an individual's decisions about his/her personal life. In relation to V2V, this is comparable to Intrusion such that its definition is sufficient.

In conclusion, privacy is a multi-faceted topic and necessitates multiple perspectives to be adequately defined. Privacy has been debated within the judicial system many times and the introduction of V2V will further complicate this issue. As the Information Age continues to push forward so will the need to educate consumers on how new technology may impede privacy. V2V communication is just one of many that will further redefine privacy.

2.12 Chapter Summary

This chapter presented a technical summary of the V2V protocol and how it can shape the future of vehicle safety through the use of particular V2V applications. These include applications, such as blind spot warning and front collision warning, that are currently available on vehicles through camera-based technologies. V2V proposes to expand on these applications with examples such as Electronic Emergency Brake Lights and Intersection Motion Assist. Each component of the BSM was presented and discussed.

An overview of the research conducted by NHTSA was given, to include: V2V privacy implications, misbehavior reports, and proposed certificate rotation methods. Modeling and simulation of BSM linking was presented along with the conclusions from that study. The next chapter of this document will utilize findings from that

work and expand on the concept of BSM linking.

Finally, a non-technical privacy law taxonomy was presented to establish a degree of understanding of privacy implications from a legal standpoint. The taxonomy was divided into four categories. These categories help describe the multiple facets of privacy to give a comprehensive viewpoint. Each category was related to V2V scenarios such that an applicable relationship was illustrated.

III. Design and Implementation Methodology

3.1 Introduction

The purpose of this chapter is to describe the methodology utilized in creating a simulation capable for studying Basic Safety Message (BSM) linking. This methodology addresses the pseudonym rotation in both candidate Public Key Infrastructure (PKI) schemes, Security Credential Management System (SCMS) and Vehicle Based Security System (VBSS). In addition, a method to create data ambiguity is presented in order to lessen the accessibility of V2V tracking capabilities. While no personally identifiable information is transmitted in BSMs, surveillance is still possible when vehicle BSMs are aggregated together. This vehicle data – Vehicular Identifiable Information (VII) – can be used to track vehicles throughout a Vehicular Ad-Hoc Network (VANET) and thus an individual person. The National Highway Traffic Safety Administration (NHTSA) currently states that no directly identifiable, or "linkable, as practical matter", or "reasonably linkable" data will be transferred. However, it was concluded BSMs could be reasonably linked given sufficient resources [25]. This leaves a gap for research and development of methods to deter BSM linking in order to preserve consumer privacy yet retain the safety benefits of Vehicle-to-Vehicle (V2V) communication.

3.2 Design Decisions and Constraints

When researching new technology, such as V2V communication, certain limitations must be considered, especially when safety is considered. Since V2V is still under development there are no official software releases of the IEEE 1609 WAVE standard. There are limited ways to obtain the standard all of which suffer from similar disadvantages. The following methods are research paths that were considered

during the design process.

The first research path considered was to implement the standard from the ground up using the IEEE 1609 standards. This method has the benefit of having complete oversight over the design process, however, it is time intensive and typically more difficult. This would leave little time for security evaluations of the standard.

The second is to obtain IEEE 1609 implementations from the academic community. These have the benefit of being open-source and more notably free. However, many of these implementations are incomplete and would need significant time and resources to finish or are implemented using obsolete versions of the IEEE 1609 standard. Additionally, network simulation software packages incorporate portions of the physical and MAC layers of the WAVE stack but omit the security and WSMP layers (IEEE 1609.2 and IEEE 1609.3 respectively). Again, because of this, significant time and resources would be required to implement the remaining WAVE stack layers.

The third method is to purchase prototype OBUs and RSUs from third-party vendors. This has the benefit of being obtainable and working out-of-the-box. However, the software running on these units are typically proprietary. Additionally, these units are designed to be installed on vehicles which is difficult to replicate in a laboratory setting.

The last method is to emulate a portion of the protocol in a simulation environment. This allows for the data being transmitted by vehicles traveling along roadways to be emulated as well as the ability to measure parameters such as distance, speed, and acceleration all within a laboratory environment. However, this approach is not without its own limitations. Since the protocol is being emulated it is not an actual implementation of the IEEE 1609 protocol. Due to this, it is crucial not fall in a cyclic design scenario where a design flaw was mitigated but was not a flaw in the protocol just the emulated portion. However, with this in mind, beneficial contributions are

still possible and this design method was ultimately chosen for this research.

3.2.1 Experimental Design.

This methodology will be split into three experiments. Each experiment tests certificate generation and the overall linkability between the BSMs of the candidate PKI systems.

1. SCMS: In the SCMS, each vehicle makes a vehicle-to-infrastructure (V2I) request for pseudonym certificates when necessary. These pseudonyms are unique to that vehicle and are temporary. NHTSA proposes the use of one pseudonym for five minutes before rotating to another out of a pool of twenty total certificates. After one week, the pool is discarded and a new pool is used. Per SAE J2735 this value is a 4 byte value allowing for 2^{32} pseudonyms. In the simulation, a group of twenty values are assigned within these windows.

2. VBSS: Under VBSS, every vehicle is part of a larger group. Vehicles use their group certificate to sign outgoing BSMs. Vehicles receiving BSM only identify the group the vehicle is a member of and not the individual vehicle. Pseudonym values are 4 byte integers and shared between other vehicles.

3. VBSS with Dithering (VBSS-D): This PKI scheme utilizes the same system as VBSS but also incorporates the data ambiguity method of dithering to non-safety critical information such as vehicle size and message ID number.

This data ambiguity method presented in this document will be dithering. The act of dithering is defined as "to act nervously or indecisively" and "add white noise" [31]. In this sense, dithering information creates indecisiveness within would-be attackers. The goal of each subsequent PKI scheme is to decrease the quantity of identifying vehicle information between itself and that of the previous scheme.

3.2.2 Assumptions.

The following assumptions are consistent across each scenario.

- V2V-capable vehicles: All vehicles simulated are V2V-equipped. Each vehicle transmits BSMs at the specified interval of 10 Hz.
- Road Side Unit (RSU) / Third-Party Receiver Access: It is assumed the RSU is a third-party receiver that is placed near a road whose only task is to collect BSMs. Third-party collectors have access to 100% of received messages.
- Basic Safety Message Requirements: The BSM is created and as specified by SAE J2735.

3.2.3 Simulation Environment.

The simulation is written within the Python programming language. To create a discrete event-based environment the library SimPy is utilized [32]. This allows for simulations to be conducted faster than "wall clock" time. Events are sorted by priority, simulation time, and lastly event identification number. For simplicity, only one event is utilized for this scenario. This event is triggered when the first vehicle in a list of vehicles enters the receiving range of the RSU. The purpose of using the SimPy python library allows for quick successive simulation iterations.

3.2.4 Simulation of BSM Transmission Session.

Vehicles simulated driving along a linear roadway. This is done by increasing the latitude BSM component of every vehicle by the distance a vehicle travels at its given speed in 100 ms (the duration between BSMs). As the vehicles travel they update every dataset with the BSM accordingly. Every vehicle's pseudonym is forced to rotate during transmission for testing purposes. Transmission of a BSM is emulated

by inserting the BSM into a dictionary. After the default duration of 100 ms has elapsed, each vehicle creates a new BSM, populates the data, and transmits it again. The standard reception radius of an RSU is 300 meters thus a RSU can receive 600 meters worth of BSMs at a time assuming the RSU is directly in the middle of the roadway.

3.3 Design Components

3.3.1 Response Variables.

- Disclosing BSM Data Elements: These are the amount of data elements within the BSM that disclose usable information to an adversary. By changing the PKI scheme each experiment, this allows us to analyze the effect these schemes have on privacy.

3.3.2 Control Variables.

- Certificate Generation: Vehicles utilizes either unique certificates or group certificates.

- Vehicle Size: Each vehicle's size is tested between static and dynamic. Dynamic testing will incorporate a range from real-world vehicle sizes to not alert potential eavesdroppers. This dynamic concept – defined as Dithering in Section 3.2.1 – is introduced to create data ambiguity between a vehicle's BSM.

3.3.3 Constant Factors.

- Vehicle Path: Vehicles are simulated to travel along a linear roadway.

- Certificates: One pool of certificates are utilized. This total signifies one weeks worth of certificates.

- Simulation Duration: Each duration are held for the amount of simulation time it takes each group of vehicles to enter RSU reception range and leave RSU reception range.
- Vehicle Quantity: Five vehicles are utilized in each test.
- RSU Amount: Each experiment will utilize one RSU. The reception range is 300 meters. This range is the expected range for Vehicle-to-Anything (V2X) devices.
- Vehicle Speed: Each vehicle maintains constant speed.

3.4 Generating the BSM

A Basic Safety Message class is constructed by following the definition and requirements established by SAE J2735 [11]. Only data that is utilized for the first part of the BSM is used. This data is the VII that will be used to link certificates to vehicles. The contents of the BSM are shown below.

- Second: The time of transmission in simulation.
- Message Count: Integer between 0 and 172. Each vehicle is initialized with a random message count.
- Temporary ID: The pseudonym certificate identifier.
- Vehicle Size: Size of the vehicle. Currently only transmits length for simplicity.
- Latitude: Latitude of vehicle. Initialized to zero and increments by accumulating the distance the vehicle travels in 100 ms. This is dependent on vehicle speed.
- Longitude: Longitude is constant yet unique for every vehicle.

- Elevation: Based off WGS84 and is constant and identical for every vehicle.
- Heading: Each vehicle is traveling the same roadway thus the same heading.
- Speed: Each vehicle is traveling at constant and near identical speeds. They are not identical as each vehicle will slightly differ from each other. They are similar to prevent vehicles from occupying the same location space.
- Steering Wheel Angle: The steering wheel angle will be zero since the roadway is assumed perfectly straight.
- Acceleration: Acceleration will be assumed near zero.

The data elements Brake Status, Transmission Status, and Positional Accuracy are not utilized.

3.4.1 Vehicle Size Determination.

The vehicle data MITRE utilized is used for these experiments [25]. This data shows that out of 308 make and model combinations, only twenty-five length to width ratios exist. These ratios are described in twenty centimeter groupings. Data that portrayed vehicle ownership composition was unavailable so data from a 2014 sales analysis was utilized [25]. Only the top ten categories out the twenty-five will be utilized as these represent almost 95% of total vehicles sold. During simulation one vehicle will be attributed to each size category. The table below depicts all twenty-five categories.

Table 2. Top 25 Vehicle Length/Width Groupings Based on Sale (2014)

Length (cm)	Width (cm)	Sale Distribution
460	180	23.23%
480	180	19.80%
580	200	12.54%
440	180	10.74%
520	200	6.63%
480	200	6.00%
500	200	5.92%
500	180	4.85%
420	180	2.70%
560	200	2.18%
520	180	1.52%
400	180	1.31%
540	180	1.01%
360	160	0.44%
460	200	0.40%
380	180	0.19%
520	220	0.16%
600	200	0.16%
440	200	0.11%
380	160	0.10%
540	200	0.09%
620	200	0.09%
260	160	0.06%
500	220	0.02%
300	160	0.01%

3.5 Certificate Linking

3.5.1 SCMS.

Upon receipt of a BSM, if the temporary ID is unique the BSM is stored under that unique ID in a dictionary. Otherwise, the BSM is stored over the last received BSM of that temporary ID. Therefore, for every unique ID, only the initial and final BSM is stored. After the simulation completes BSM matching is performed. Every initial message and final message are compared against each other. The comparison projects what each final BSM data would have been 100 ms in the future and compares

it to that of the initial BSM. If the projected BSM matched the initial BSM then it can be assumed the two BSMs originated from the same vehicle under two unique pseudonyms - illustrating a pseudonym rotation.

3.5.2 VBSS.

Under the VBSS, pseudonyms are no longer unique and are now group IDs. Since the pseudonym is no longer unique a new key has to be utilized for linking purposes. Thus, a dictionary can no longer be used as there are no unique non-volatile information being transmitted. Every BSM is now recorded the use of group pseudonym and vehicle size filters are utilized. Again, if the projected BSM data matches any of the initial BSMs then it can be assumed the two BSMs originated from the same vehicle.

3.5.3 VBSS-D.

In the MITRE study [25], it was determined that quasi-identifiers such as vehicle size and other data could be used to track vehicle certificates' even when certificate changing was implemented. It was shown that the longer the lifetime of a certificate the higher the probability that tracking was possible. This work proposes a quasi-identifier ambiguity method that dithers the value of these quasi-identifiers when applicable. In doing so, this decreases the amount of quasi-identifiers eavesdroppers can use as linking agents. It should be noted that, this ambiguity generation is only be possible when V2V applications are not depending on the quasi-identifiers for safety purposes. Otherwise, false information could be received by a V2V device and recognized as legitimate. This could lead to unforeseen consequences such as collisions and other detrimental effects.

Thus, the experiment uses the same certificate algorithm as VBSS but will incor-

porate dithering on the non-safety BSM data components. The dithered components are vehicle size and message ID. Vehicles are scheduled to randomly broadcast vehicle size with a range of 270 - 520 (cm). This window range of the smallest and longest length of current production vehicles in North America. Message ID will randomly be chosen when the vehicle changes to a new pseudonym. Per SAE J2735, non-sequential message IDs imply messages were lost in transmission, thus, randomly changing message ID is not possible. Positional Accuracy is not dithered because fluctuating the accuracy of the reporting vehicle would create unnecessary false-positive and false-negative alerts. By introducing the notion of dithering, the usefulnesses of BSM contents to a third-party collector is reduced increasing the level of effort necessary for a collector to link pseudonyms.

3.6 Summary

The objective of this chapter is to demonstrate that using V2V BSM tracking is accessible in a reasonably and practical manner. By building off the work of the MITRE study and adding ambiguity generation this accessibility to V2V tracking is reduced. The risk of location tracking may never be eliminated due to the contrasting nature of safety and privacy. However, the ability to decrease the feasibility of third-party collectors to track vehicles is possible. This chapter discussed design methods and constraints as well as test variables and factors to test dithering of BSM attributes. Python and the SimPy simulation library was used to create the synthetic environment utilized throughout this chapter. The following chapter analyzes the effects of BSM linking between SCMS, VBSS, and VBSS-D.

IV. Analysis

4.1 Introduction

The purpose of this chapter is to evaluate and analyze the Basic Safety Message (BSM) eavesdropping simulation presented in Chapter III. This chapter is divided into different section s that evaluates a different aspect of the proposed tracking deferral algorithm. The first section explores the implications of Vehicle-to-Vehicle (V2V) communication and will introduce topics that will be discussed throughout this chapter. The second discusses the linking algorithm and its effectiveness to the three different experiments from Chapter III. A Vehicular Ad-Hoc Network (VANET) evaluation metric is presented that illustrates the privacy, safety, and security trade-offs that need to be considered when implementing V2V communication. This criteria is applied to four different subsystems: a non-VANET environment, a Security Credential Management System (SCMS)-based environment, and a Vehicle Based Security System (VBSS)-based environment, and lastly, VBSS with Dithering is discussed along with VBSS as the core concepts are identical. In addition, the Common Vulnerability Scoring System is utilized to apply a quantitative metric to each Public Key Infrastructure (PKI) scheme centered around location tracking. The final section introduces policies and recommendations in order to thwart certain third-party V2V tracking.

4.1.1 Adversaries.

Throughout this chapter, two types of adversaries are presented. The first, an unsophisticated eavesdropper, is the equivalent of a burglar is considered. In theory, this adversary places a single BSM receiver within a neighborhood. The transmission range of a typical device is 300 meters; therefore, an adversary needs to be able

to collect BSMs from each vehicle within the radius of the receiver. Vehicles begin transmitting messages as soon as the vehicle is placed in gear resulting in vehicles disclosing the latitude and longitude of the vehicles at each residence within the neighborhood. In doing so, a link can be formed between individual vehicles and residences. Over time, the actor can create a temporal pattern for each vehicle at every household and use it to conduct numerous crimes. This act of eavesdropping is referred to as unsophisticated because the linking occurs between data within a single BSM and data that is non-BSM derived (in this case the latitude and longitude of a house).

The second type of eavesdropper is that of the sophisticated eavesdropper. Unlike the unsophisticated eavesdropper, this actor has the resources to place BSM receivers across large distances; enough such that every BSM transmitted from every vehicle would be collected. This actor also has the computational ability to analyze every BSM collected and link BSMs that belong to the same vehicle. Thus, precise location history can be determined for each and every vehicle. A study from 2009 shows that using only work and home locations the identity of an individual could be revealed [33]. The organized collection of BSMs not only reveal home and work locations but also every location the vehicle visited including schools, doctor offices, and anywhere in-between. A comprehensive pattern of life could result for every vehicle from this data.

The motives for the sophisticated eavesdropper are more complex than that of the unsophisticated eavesdropper. Actors that have resources and abilities to be sophisticated would most likely be state-level organizations and large corporations. Traffic laws such as speeding, red light running, and other moving violations could be enforced through V2V communication alleviating some responsibility from law enforcement officers. This concept is similar to cameras that capture red light runners.

One foreseeable circumstance for V2V monitoring is speed limit enforcement throughout construction zones, school zones, and other specialized zones. Large corporations could collect BSMs to determine where to locate businesses in high congestion areas to maximize profits or sell the data collected to other corporations.

Note, the term Vehicular Identifiable Information (VII) and quasi-identifiers will be used throughout this chapter. VII discloses information that can be tied to specific vehicles. Where, unique pseudonyms are an example of VII. Quasi-identifiers are BSM data that when aggregated together reveal vehicle identity. Vehicle size, message count, time stamp, and location are forms of quasi-identifiers.

4.2 Implications of Dithering

In addition, this chapter analyzes the ability for advanced adversaries to track individuals under the two PKI schemes presented by the National Highway Traffic Safety Administration (NHTSA) and VBSS with dithering. It is noted that dithering is not possible when the dithered information is required for safety applications. One such scenario is the notion of autonomous intersections where true vehicle size, speed, and path history are required to be transmitted for at least the amount of time it takes a vehicle to arrive, enter, and exit an intersection. Dithering vehicle information could cause potential accidents or unnecessary congestion. A response to this scenario and others like it would be to transmit information modified by a constant factor in order to deter vehicle identification without crippling V2V effectiveness. For instance, in autonomous intersections, vehicle's should only be allowed to increase their reported size by a certain factor and not decrease as this could lead to intersection overbooking by the Intersection Manager (IM). Other information, such as speed, would not be able to be dithered as speed is used by a IM to deliver reservations and thus true speed is required to be transmitted.

A second scenario where dithering would be not possible is high speed multi-lane freeway scenarios especially during rush hour when freeways are highly congested. During this scenario it is crucial for vehicles to maintain near constant speed to prevent the "slinky effect" where vehicle spacing may compress or expand. With dithering enabled, vehicles broadcasting fluctuating size, speed, and location would inevitably cause events such as the "slinky effect" needlessly which in turn under utilize the infrastructure and increase commute times which in turn frustrates drivers. This would not benefit public opinion of V2V communication. In addition, rush hour driving can include last minute lane changes, merging, and swerving from debris. If a vehicle transmitted dithered size it could trigger false positives in surrounding vehicles leading the driver to believe the V2V technology was misbehaving, therefore decreasing the trust level of the driver. A response for these scenarios would be to disable dithering at freeway speeds and at high capacity VANETs.

4.3 Linking Algorithm

4.3.1 Simulation Results.

Given the assumption of 100% of BSMs collection and the five vehicles utilized across each of the three simulations results in the linking of each vehicle's BSMs. However, the differences in each simulation reside in the amount BSM parameters at the disposal of third-party collectors to link BSMs as well as the level of effort necessary for third-party collectors to create that link. The following sections depict what data each simulation utilizes. For each simulation, a flowchart is given to depict how BSM linking is achieved along with the relevant disclosing BSM data contents.

4.3.2 Pseudonym Linking Algorithm.

The act of BSM linking is defined as connecting one or more BSMs to an individual. This is done by using the spatial and temporal data elements within each BSM. If successful, BSM eavesdroppers will be able determine vehicle owner identity and complete location history of that individual. Dictionaries allow for entries (values) to be stored under unique items (keys) to increase efficiency. The dictionary is populated in real time as the receiver receives BSMs from passing vehicles. If the key is not in the dictionary a new entry is created using the pseudonym as the key and the BSM is inserted as the value. If the key is in the dictionary the most recent BSM in the values is overwritten unless that BSM is the initial message. Therefore, only the first received BSM and last received BSM are stored for any one key. The data within the first messages are compared to the final messages and any matches are determined. The linking for each scheme is discussed in the next section along with a flowchart to depict the linking process. All three of these algorithms result in complete matching of BSMs due the spatial and temporal elements. However, the level of effort and computational effort is increased between them.

4.3.3 Linking Effectiveness.

The SCMS scheme allows for multiple VII pieces to be tied to vehicles. The pseudonym is the largest perpetrator since it is unique to a single vehicle. With SCMS, the dictionary key will be each unique pseudonym. When two BSMs are compared with two different pseudonyms (marking a potential pseudonym rotation) the other elements of the BSM are compared to confirm or deny pseudonym rotation. This is done by projecting the first BSM contents 100 ms in the future. Thus, if the projected BSM contents and final BSM contents are alike, then a link between pseudonyms can be formed. Once matches are identified the unique pseudonyms

are now linked negating the purpose of rotating certificates. The unsophisticated tracker does not have to perform BSM linking as their motives are to link vehicles to specific locations (home, work, etc.). Thus, unique pseudonyms do not deter this action. It also does not prevent sophisticated trackers from tracking through linking unique pseudonyms by using BSM contents such as vehicle size, quasi-identifiers, and vehicle location. Even rotating through certificates each week would only require the sophisticated tracker to perform the linking process every week. The BSM contents that are utilized in linking are unique pseudonym, vehicle size, and spatial/temporal elements.

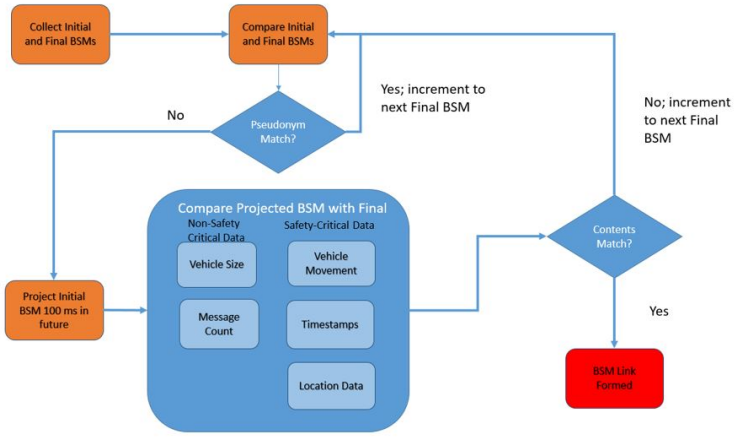

Figure 10. SCMS BSM Data Linking Flowchart

VBSS attempts to mitigate the linkability of unique pseudonyms by the use of group pseudonyms. Since pseudonyms are common between vehicles the use of a dictionary is no longer possible. This technique decreases the amount VII a vehicle discloses but, in turn, transforms the pseudonym from VII as it was under SCMS to a quasi-identifier. Thus, the unsophisticated tracker will still be able link locations to specific vehicles. The sophisticated tracker will be able to utilize the vehicle size, vehicle location, and other quasi-identifiers. This is shown in the linking algorithm by filtering messages by group pseudonyms, then filtering by vehicle size. And lastly,

location, movement, and timestamps are filtered creating individual patterns for each vehicle. Group pseudonyms prevent vehicles from disclosing their individual identity yet aggregation of other quasi-identifiers will still lead to BSM linking and thus location tracking. However, the VBSS scheme does increase the level of sophistication and effort required by eavesdroppers to successfully perform BSM linking. The BSM contents that are utilized in linking are group pseudonym, vehicle size, and spatial/temporal elements.

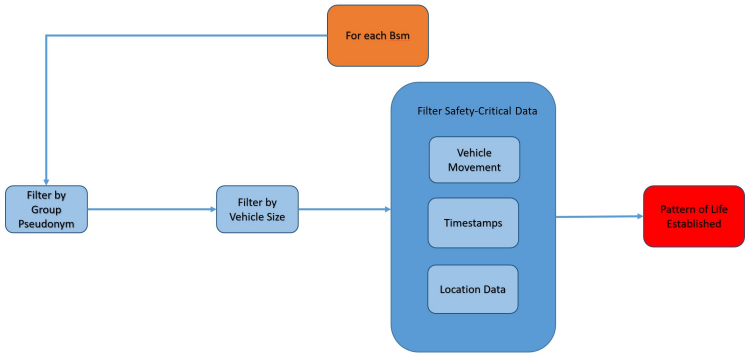

Figure 11. VBSS BSM Data Linking Flowchart

VBSS with Dithering utilizes the same VBSS implementation but attempts to further decrease the amount of quasi-identifiers available for use in BSM linking. By dithering the vehicle size in every BSM, VBSS with Dithering (VBSS-D) decreases the usable quasi-identifiers to only vehicle location (depicted as latitude, longitude, and elevation), the group pseudonym, and the time stamp. This is shown below in Figure 12 as a bypass around the Vehicle Size filter. Again, unsophisticated adversaries will be able to link vehicles to specific locations. Sophisticated trackers will be able to link BSMs through use of safety-critical information such as vehicle movement, time stamps, and location yet by removing all non-safety usable VII and quasi-identifiers has decreased the confidence of linking and forced the sophisticated tracker to pursue more sophisticated tracking means. By doing so, VBSS-D prevents BSM linking from

all except the most sophisticated adversaries. The BSM contents that are utilized in linking are group pseudonym and spatial/temporal elements.

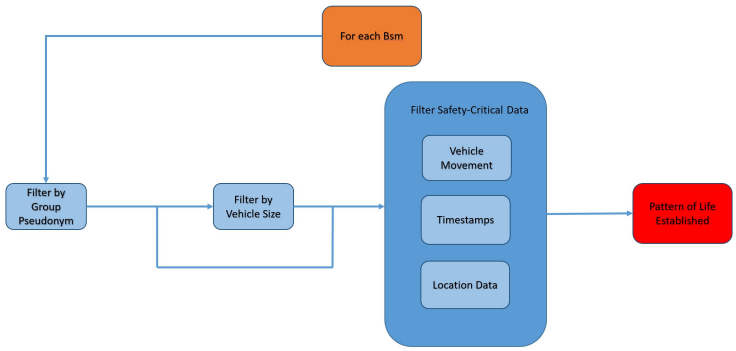

Figure 12. VBSS-D BSM Data Linking Flowchart

4.4 VANET Metric Classification Overview

A VANET metric classification will be presented to analyze and compare proposed PKI schemes and depict how Dithering improves these methods. In addition, these evaluation criteria is not to say which scheme is better or worse but rather to inform consumers that inevitably have the decision of purchasing V2V-equipped vehicles in the near future. The VANET metric classification broken into five subcategories: Cost, Privacy, Safety, Efficiency, and Stability.

4.4.1 Scoring System.

The Common Vulnerability Scoring System (CVSS) provides a means to classify and quantify vulnerabilities of software and hardware [34]. By doing so, CVSS can allow its users to properly analyze and manage their respective networks. CVSS is an open framework allowing for transparency and ease of explanation for how each and every measurement is produced. CVSS is categorized into three sections: Base, Temporal, and Environmental. The base creates a fundamental score that is then

modified by temporal or environmental elements, if applicable. For V2V purposes, only the Base category will be utilized.

The Base category is split into two subsections: exploitability and impact metrics. Each of these subsections are composed of separate components that are chosen based on the network being analyzed. Both subsections and their components are listed below.

Exploitability

- Attack Vector: Context by which the vulnerability is possible [Network, Adjacent, Local, and Physical]
- Attack Complexity: Conditions that must exist for the attack to occur [Low, High]
- Privileges Required: Privileges the attacker must possess before execution [None, Low, High]
- User Interaction: Requirement of a user, other than the attacker, must participate in order for successful execution [None, Required]
- Scope: The ability for a vulnerability in one component to impact resources beyond its authorization [Unchanged, Changed]

Impact metrics

- Confidentiality Impact: Impact to the confidentiality of information [High, Low, None]
- Integrity Impact: Integrity of information after a successful exploit [High, Low, None]
- Availability Impact: Availability of a component after a successful exploit [High, Low, None]

4.4.1.1 Cost.

With any legislative mandate, cost is a critical item. V2V communication will likely be initially deemed a luxury and therefore only available in high-end vehicles. Any rule making determined partially by public acceptance and exorbitant prices will hinder public support. In addition to consumer cost, this category also incorporates costs that are indirectly paid for by the consumer such as back end infrastructure and other necessary components.

4.4.1.2 Privacy.

V2V privacy, in this context, is the ability of third-party listeners to aggregate information together and create a pattern of life for individual vehicles within a VANET. NHTSA strives to push a "privacy by design" approach for V2V application designers and the rule of no "reasonably linkable" data to be transmitted. However, as described above, it is possible for eavesdroppers to use meta-data to create profiles of individuals. This component is arguably the most important as data analytics is an enormous field and many corporations are eager for V2V to become available – regardless of the benefit to the consumer. Referring back to the privacy law taxonomy, this topic will refer to information disclosure and processing.

4.4.1.3 Safety.

The main purpose to V2V is improve driver awareness with the objective of decreasing accidents. In many cases, however, the increase of safety typically leads to a decrease of privacy. This has been accentuated in the past decade and half at airport terminals. After the terrorist attacks of 9/11, travelers have been subjected to more invasive searches in the interest of increased safety. However, unlike airport terminals, V2V will be integrated into consumers everyday lives. Consumers drive their

vehicle daily where the average consumer may fly a few times a year so the trade-off of privacy is reasonable for airport safety.

4.4.1.4 Efficiency.

In addition to safety, V2V also promises increased efficiency. By informing drivers of congestion, V2V allows drivers to use alternate routes to their destination. This decreases the amount of time the vehicle would be running decreasing the amount of fuel consumed. In addition, traffic congestion is also reduced since more vehicles would be taking alternate routes.

4.4.1.5 Stability.

The final component of this criteria is stability. This refers to the stability of the VANET of how resilient it is in the event of malicious, misbehavior, and malfunction events. In addition, ease of certificate revocation is considered within this category as the mishandling of certificates during the revocation process may lead scenarios where vehicles trusting revoked certificates.

4.4.2 VANET Metric Classification and CVSS Application.

These evaluation criteria are applied to three different subsystems. First, it is utilized to describe non-V2V equipped vehicles to give a baseline for the other two systems to be compared against. Secondly, the SCMS-based VANET where unique pseudonyms are utilized is analyzed. The final section describes both VBSS and VBSS-D as their PKI components are the same. To conclude each discussion, the Common Vulnerability Scoring System (CVSS) components are presented.

4.4.2.1 Current Infrastructure (Non-V2V).

This evaluation covers aspects of VANET implementations and thus the current cost to the consumer for V2V insignificant. Non-V2V privacy was discussed previously in Chapter II with the discussion of NHTSAs Privacy Impact Assessment. In the assessment, NHTSA discusses current tracking vehicle techniques such as physically following a vehicle, installing a GPS tracker, and accessing cell phone history and other databases. Out of the methods listed by NHTSA physically following a vehicle is the most accessible method. This requires a ratio of one tracking vehicle for every victim vehicle. However, these tracking techniques are only applicable when a specific vehicle is the desired target. They do not account for mass systematic vehicle tracking. Currently, this is probable through the use of individual mobile phone applications such Google Maps or similar applications. In fact, Google currently utilizes individuals' mobile phone location data to display traffic congestion However, the individual can opt out of this by turning location services off and individuals who do not opt-out have to trust Google not to mishandle their data. In addition, the Supreme Court case, *United States vs Knotts* [30], ruled that once one leaves his/her home, there is no reasonable expectation of privacy. This case, however, occurred at a time when connected vehicles were not a possibility.

Safety is a critical component of vehicle design and has been heavily influenced by NHTSA studies and mandates in the past. Currently, many vehicle safety devices are reactive in nature such as seat belts and airbags deploying safety mechanisms milliseconds after a crash occurs. Recently, technology such as radar and LiDAR has become more standard and has introduced active vehicle safety applications such as lane keep assist, brake assist, and adaptive cruise control. So overall, vehicle safety continues to improve as technology improves and becomes more standard across vehicle lineups.

Efficiency has also become a critical component of vehicle design as manufacturers are subject to emission testing and more consumers in general strive to lessen their environmental impact. Currently, emissions are reduced by designing more fuel efficient vehicles such as utilizing hybrid engine designs, increased vehicle aerodynamics, and routine vehicle maintenance (e.g. proper tire pressure, clean air filters, etc.).

Lastly, current vehicle network stability has become increasingly unbalanced as recent vehicle technology has been susceptible to attacks [35]. However, many of these attacks require sophisticated attackers and physical access to accomplish.

Table 3. Non-VANET Tracking CVSS Metric

Exploitabiltiy	**Classification**	**Impact Metrics**	**Classification**
Attack Vector	Physical	Confidentiality	High
Attack Complexity	Low	Integrity	None
Privileges Required	None	Availability	None
User Interaction	Required	Scope	Unchanged
Scope	Unchanged	–	–

The attack vector is classified as Physical such that the most prominent non-V2V tracking methods (following, GPS-transmitter, etc.) require physical access to the target vehicle. Attack complexity is low because non-V2V tracking methods are relatively low effort. No privileges are required to perform these methods, and user interaction is required as they need to be traveling in a vehicle to provide tracking capabilities. Performing tracking methods does not affect scope in either category. Confidentiality is classified as high since these methods reveal 100% location history revealing other sensitive information. Availability and integrity remain unchanged. The final CVSS score for non-VANET tracking is 4.3 (medium).

4.4.3 Security Credential Management System.

Under the proposed SCMS-based VANET, vehicles will have unique certificates and the PKI implementation will utilize a split entity concept where no one entity

will hold enough information to identify individual nodes within the VANET. Cost will be broken down into two subcategories. The first will be the cost that will be directly paid for by the consumer and the second will be the cost of installing and operating the SCMS infrastructure. According to a 2014 study conducted by NHTSA the total cost per vehicle in 2022 would be roughly $350 [36]. This cost is projected to decrease to just above $200 over a thirty year time period. This cost can be further broken down into four subcategories: equipment costs, fuel economy costs, security credentials cost, and communication costs. The On-Board Unit (OBU) is reported to cost the majority of the total cost coming in at around $330. By adding the OBU to the vehicle, fuel costs are projected to $9 to $18 over the lifetime of the vehicle.

NHTSA projects a cost of $8.50 for securing communications across vehicles. However, they base this assumption on the belief of a low probability of misbehavior due to a predicted low initial penetration rate of V2V. In the opinion of the author, this mentality would reflect poorly on the adoption rate of V2V thus crippling the safety purposes of V2V communication. Lastly, NHTSA estimates a fee of $3.14 attributed for the cost of the SCMS. Based off these estimates, total annual cost is predicted to be between $2.2 billion and $5.0 billion. NHTSA says that the "breakeven" point (the point where the value safety benefits exceeds the costs to consumers and manufacturers) is between 2029 and 2032 depending on market penetration. At $2.2 billion – $5.0 billion per year, convincing legislature that V2V communication would require $22 billion – $50 billion investment before monetary benefits are realized would be an extremely difficult hurdle. NHTSA also bases this analysis on human drivers where it is exceedingly likely that autonomous vehicles will become standard. Waymo, Alphabet's driverless car company, has recently deployed driverless vehicles in Phoenix, Arizona [37].

Concerning privacy, NHTSA states that the SCMS design will make it difficult for

third-parties attempting to track vehicles and will need "requires significant resources and effort to do so" [1]. As illustrated previously in this chapter, unique pseudonyms provide a relatively simple way to perform BSM linking. In the author's opinion, NHTSA is underestimating the abilities and resources of third party organizations. Home and work location pairs are sensitive information as it was demonstrated by disclosing home location and work location a majority of Americans could be identified [33]. V2V communication would not only disclose home and work locations but every other location a vehicle has traveled allowing for a comprehensive pattern of life. The current system does not prevent unsophisticated trackers such as burglars where their goal is to determine when vehicles leave or exit, nor does it prevent sophisticated trackers from creating profiles for each V2V equipped vehicle.

V2V communication introduces proactive safety monitoring applications discussed in Chapter II. These are meant to alert the driver of potential hazards in effort to prevent collisions from occurring. Proactive safety mechanisms have been introduced in vehicles, such as Light Detection and Ranging (LiDAR), but these devices are limited by line-of-sight. V2V expands upon these systems by allowing numerous additional safety applications, and possibly, in the not-so-distant future, autonomy. In this sense, V2V and vehicle-resident systems can act as means to checks and balances system where one systems verifies the other systems findings and vice versa.

V2V also promises the ability to increase efficiency. This is not done by improving the efficiency of vehicles but rather the efficiency in how the vehicles are driven. This can be done by a V2V alert informing the driver of congestion along his/her predefined route. This would allow the driver to take a detour from the congested route decreasing the amount time the driver would spend in traffic and reduce the amount of traffic at the area of congestion. Emissions can also be reduced from the notion of platooning. Platooning allows for multiple vehicles to travel together within

close proximity to utilize the reduction of drag caused by the lead vehicle. However, platooning requires near 100% adoption rate of V2V thus initial benefit is limited.

Lastly, the stability of the SCMS is uncertain. NHTSA states V2V will have a low initial adoption rate such that there is little reward for malicious entities to act. This is a favorable statement yet this outlook may prove to be naive. The proposed SCMS is the most complex PKI implementations in terms of size, infrastructure entities, and revocation requirements if created. The DoD PKI system is currently one of the largest PKI systems in implementation with fifty million certificates [38]. Many of which are long term such as the certificates used for Common Access Cards which are utilized typically for three years [39]. SCMS will have to support certificates for three hundred million vehicles – a conservative estimation. At twenty certificates per vehicle per week the SCMS will have to support six *billion* certificates each week assuming full V2V penetration. Supporting such a complex system is staggering even without malicious activity. Introducing malicious actors and the task of preventing security breaches while maintaining privacy of non-malicious drivers is overwhelming. In addition, certificate revocation is also an intense hurdle to overcome as well. Under the SCMS scheme, vehicles create misbehavior reports and send them to the misbehavior authority for analysis. The misbehavior authority analyzes them and then determines whether to revoke or not revoke the misbehaving certificate. The time for this process to occur will likely allow misbehaving vehicles to perform the misbehavior action numerous times.

The attack vector now has changed to Adjacent as an adversary needs only a V2V receiver to obtain BSMs and send them to a database for processing. Attack complexity is two part; under unsophisticated adversary the attacker needs only one V2V receiver to listen in on BSMs in order to gain information to complete his/her goal thus complexity is low. However, a sophisticated adversary needs a network

of V2V receivers to collect BSMs and then the software and hardware necessary to perform pseudonym linking thus complexity is high. Again, privileges and user interaction remain the same as non-V2V tracking. Confidentiality also remains high as adversaries will be able to determine location history as well as vehicle size and linking unique pseudonyms all which reveal sensitive information about the individual. In addition, Availability and Integrity are classified as None as tracking does not affect the integrity of BSMs and BSM are already readily available for collection. These results are tablized below in Table 4. The CVSS score for SCMS tracking for the unsophisticated adversary is 5.7 (medium) and 4.8 (medium) for the sophisticated adversary.

Table 4. SCMS Tracking CVSS Metric

Exploitabiltiy	**Classification**	**Impact Metrics**	**Classification**
Attack Vector	Adjacent	Confidentiality	High
Attack Complexity	Low* / High**	Integrity	None
Privileges Required	None	Availability	None
User Interaction	Required	Scope	Unchanged
Scope	Unchanged	–	–

4.4.4 VBSS and VBSS with Dithering.

The evaluation will be applied to VBSS and VBSS with Dithering concurrently since both are similar in nature. Where the differences reside will be illustrated. In addition, the CVSS score will only be applied to VBSS with Dithering as this scheme incorporates all aspects from VBSS alone. VBSS is not as mature as SCMS thus not as much cost analysis has been meticulously done as is the case with SCMS. However, much of the price can be inferred from VBSS requirements. OBU hardware can be expected to be more expensive than hardware under the SCMS scheme as VBSS incorporates cryptographic processes that are performed by the OBU. Apart from OBUs, VBSS would require less internal entities than that of SCMS reducing

operation. In addition, if a VBSS system was implemented, Road Side Unit (RSU) interactions are reduced as vehicles pseudonym requests are less frequent than the SCMS scheme. This sections applies to both VBSS and VBSS with Dithering.

VBSS reduces the amount of VII since pseudonyms are no longer tied to an individual vehicle but are now tied to a group. However, vehicle size, speed, and location are still broadcasted allowing linking. The use of group pseudonyms would disable unsophisticated trackers who lack the resources to aggregate BSMs. BSM linking using vehicle size along with group pseudonyms time stamps enable sophisticated trackers to form patterns of life for each vehicle through meta-data such as where a vehicle travels throughout the day, time it spends at each location, and other techniques.

VBSS with Dithering strips all forms of non-safety critical VII but cannot remove location transmission without crippling the safety applications of V2V. Thus, VBSS with Dithering allows only highly sophisticated trackers the ability to track but still allows tracking nonetheless. The evaluation criteria aspects of safety and efficiency remain largely unchanged under VBSS than that of SCMS. Since PKI does not affect the way safety applications and other applications operate the determination is fair.

Concerning stability, VBSS has less internal entities as than that of SCMS the system is less complex however size is still a factor. Thus, many of the same conclusions of SCMS apply to VBSS. However, revocation increases in complexity relative to SCMS. In SCMS, if a certificate was determined to be misbehaving only that single certificate needs to be added to the revocation list. In VBSS, if a vehicle is misbehaving, the entire group pseudonym for which that vehicle belongs to would need to be revoked. Some research has proposed implementing primary and secondary group pseudonyms for cases such as this [22]. However, this also doubles the necessary amount of certificate required to be maintained increasing complexity to an already complex PKI system.

Concerning VBSS all categories are identical to the SCMS CVSS analysis except for Confidentiality. This metric has been downgraded to Low as non-safety essential VII has now been deemed unusable through dithering and group pseudonyms. Thus the CVSS score for unsophisticated and sophisticated adversaries 3.5 (Medium) and 2.6 (Low). VBSS and VBSS-D are listed under identical scores for Confidentiality since there are only three options (None, Low, High). If the CVSS Confidentiality category had finer granularity it would be able to represent each subsystem in greater detail. These results are shown below in Table 5.

Table 5. VBSS with Dithering Tracking CVSS Metric

Exploitabiltiy	**Classification**	**Impact Metrics**	**Classification**
Attack Vector	Adjacent	Confidentiality	Low
Attack Complexity	Low* / High**	Integrity	None
Privileges Required	None	Availability	None
User Interaction	Required	Scope	Unchanged
Scope	Unchanged	–	–

The metrics for all three systems are shown in the table below. Based off these scores, VBSS-D provides the best score (lower is better) in relation to information disclosure to an adversary. It should be noted that the CVSS was not designed with VANET in mind. In addition, CVSS should not be compared by score alone. The context to which the score was determined should be taken into account before critical decisions and design alterations are made.

Table 6. Scores of all VANET Schemes

System	**CVSS Metric**
Non-VANET	**4.6** (medium)
SCMS	Unsophisticated: **5.7** (medium) & Sophisticated: **4.8** (medium)
VBSS with Dithering	Unsophisticated: **3.5** (medium) & Sophisticated: **2.6** (Low)

4.5 Policies

This section introduces policies and best practice methods for V2V communication in order to deter adversaries from utilizing V2V communication for malicious purposes. The first policy presented is in attempt to prevent unsophisticated adversaries from determining home locations of individuals. Currently, NHTSA proposes vehicles begin transmitting BSMs within two seconds after the driver places the vehicle in gear (forward or reverse). In other words, NHTSA "believes the vehicle should begin transmitting before the vast majority of drivers begin driving the vehicle". However, with BSMs transmitting location within 1.5 meter accuracy eavesdroppers will easily be able to determine driveways and parking spots of transmitting vehicles which would lead to disclosure of owner identity. As stated earlier, such information (e.g. work-home locations pairs) can and should be classified as personally identifiable information [33].

If vehicles did not begin transmitting BSMs until a speed of 15 mph was reached this would prevent vehicles from disclosing point of origin (e.g. home, work, etc.) to a high degree of precision. It would allow vehicles to travel far enough away from their start location such that exact residences were not revealed. However, this would only prevent point of origin locations from being revealed and not destination.

To prevent disclosure of destination (i.e. home, work etc.) vehicles can be programmed with work and home locations (similar to how GPSs function) such that when the vehicle enters a certain radius in relation to either location V2V transmissions would cease. The safety aspects of halting transmissions should be properly evaluated before being deployed.

4.6 Summary

The goal of this chapter was to analyze the methodology presented to determine the feasibility of BSM linking and ultimately the candidate PKI schemes NHTSA has proposed for V2V communication. The notion of dithering non-safety critical BSM data was analyzed to increase the sophistication necessary to link certificates. The use of dithering VII such as vehicle size and the use of group pseudonyms eliminates the usability of certain VII by eavesdroppers. However, highly sophisticated adversaries can utilize safety-critical BSM data such as location, speed, acceleration, and even steering wheel angle to determine vehicle location history. This history combined with other forms of meta-data such as where vehicles travel and for how long can allow these adversaries determine patterns of life revealing individual identity.

A VANET Metric Classification was presented that discussed the ramifications focusing on five areas specifically cost, privacy, safety, efficiency, and stability. This evaluation criteria was applied to each PKI scheme and highlighted strengths and deficiencies within these five categories. In addition, the CVSS was applied to each PKI to provide a quantitative metric for comparing these schemes. Lastly, polices and best method practices were presented to mitigate the collection of vehicle departure and destination locations.

V. Conclusion

5.1 Introduction

As technology continues to advance, vehicle safety should advance along with it. In the case of Vehicle-to-Vehicle (V2V), it is crucial for consumers to understand any and all repercussions of new technology they purchase and entrust with their life.

5.2 Summary

This thesis introduced the Wireless Access in Vehicular Environments (WAVE) protocol which makes V2V communication possible. Safety applications were presented that highlighted how V2V could benefit drivers and possibly create a path to fully autonomous vehicles. Current and past research was presented, mostly conducted by the National Highway Traffic Safety Administration (NHTSA), that showcased the current state of the technology and introduced some concerns about vehicles self-disclosing information. Most notably, the ability and consequences of eavesdroppers linking two pseudonyms together through Basic Safety Message (BSM) contents effectively revealing location history of every V2V-equipped vehicle.

Three Public Key Infrastructure (PKI) schemes were explored to show how eavesdroppers could link two BSMs regardless of pseudonym. The purpose of each successive scenario is to decrease the amount of information available to the eavesdropper yet retain V2V functionality. The first scenario was the Security Credential Management System (SCMS) PKI, which is NHTSA's current leading implementation. The scheme utilizes unique pseudonyms for every vehicle which rotate every five minutes from a pool of twenty certificates. Thus, to link two BSMs with dissimilar pseudonyms, an eavesdropper could project the future location of the latter BSM by calculating the location data and speed data of the first BSM. If the projected BSM matched the

latter BSM then it could be determined that the two pseudonyms originated from the two vehicles.

The second scheme was the Vehicle Based Security System (VBSS). This PKI implementation utilizes group pseudonyms. Vehicles do not disclose individual identifiers but only the identity of the group of which the vehicle belongs. By doing so the amount of information used for linking BSMs is decreased and thus increasing the sophistication required by the eavesdropper. Linking is still possible through the use of vehicle size, speed, and location parameters.

The third scenario utilizes the VBSS with Dithering (VBSS-D). This scenario utilizes the group pseudonyms of VBSS along with the data ambiguity method of dithering. This allowed the randomization of the non-safety critical information transmitted from each vehicle. By implementing dithering the only information at the disposal of the eavesdroppers is the safety critical information which are speed, time, and location parameters. By doing so, dithering allows only highly sophisticated eavesdroppers to link BSMs.

A Vehicular Ad-Hoc Network (VANET) metric classification was applied to these three schemes as well as the current state of vehicle environments. The five categories of the classification that were introduced were safety, privacy, efficiency, cost, and stability. These categories were chosen to evaluate the effects of V2V communication for better or worse. In addition, the schemes were quantified using the Common Vulnerability Scoring System (CVSS) to establish scores to simplify comparisons between schemes.

5.3 Contributions

The viability of maintaining location privacy while retaining safety applications was presented throughout the course of this thesis. The fundamental information

that is utilized by every V2V application (location, speed, and acceleration) are also essential in linking BSMs. Thereby, absolute prevention of BSM linking was shown to be not possible. However, through the use of group pseudonyms and data ambiguity methods, such as dithering, the technical sophistication required by third party collects is increased. In doing so, consumer privacy loss risk mitigation is reduced enough to fit within NHTSAs decree that no "reasonable linkable" data is permitted to be transmitted.

5.4 Counterarguments

5.4.1 Privacy Is Already Forfeited.

The argument can be made that consumer information is already being obtained through means other than V2V communication. This section will explore alternative methods that enable location tracking and how they compare to V2V communication. The first method are RFID devices that are commonly utilized for toll passes. Radio-frequency identification trackers can collect when and where vehicles travel establishing a pattern of life [40]. On a larger scale, Automated License Plate Readers (ALPRs) record license plate numbers along with location, time, and date of scanning. Attached to light posts, bridges, and police vehicles ALPRs have the ability to create a pattern of life for every vehicle in their line of sight [41]. On an even larger scale location history can be tracked through mobile device applications such as Google Maps [42]. These applications can reveal high fidelity location history as mobile phones are typically carried on a person at all times. However, these scenarios all have mitigations that a consumer could execute to alleviate tracking capabilities. RFID toll passes are not necessary to utilize toll roads, and while the trade-off is an inconvenience to the driver; the driver has to make the conscious decision of opting-in for device use. APLRs can be defeated through the use of photo-reflective license

plate covers - aside from questioning legality. Mobile device applications, similar to RFID toll passes, require the user make the conscious decision to opt in to disclosing location information. Each of the scenarios involve tracking individual vehicles albeit on differing scales. V2V communication would allow for comprehensive information gathering on every vehicle that traveled within proximity of a receiver and there are no preventative measures against it. Thus, in the opinion of the author, one should not accept the notion that individual privacy is already forfeited.

5.4.2 Necessity of Message Authentication.

Whichever PKI design NHTSA pursues, it will become one of the most complex and distributed PKI schemes in existence. In the case of SCMS, much of this complexity is a result of the privacy by design approach. NHTSA claims through the use of certificates recipients will be able to determine that a BSM originated from a trustworthy source and thus the information contained within the BSM is factual all while remaining anonymous. This notion counteracts the fundamental purpose of authentication; the act of confirming data integrity by confirming a senders identity [43],[44]. In a V2V environment, where messages determine vehicle paths, this can result in costly and irreversible actions.

This thesis has discussed NHTSAs leading proposed PKI scheme SCMS and the alternative of VBSS. The difficulties surrounding each scheme have been presented in addition to the misapplication of the usage of PKI message authentication. Considering these issues together raises the question of the necessity of requiring message authentication with V2V. From an individual vehicle point of view, the majority of BSMs received can be ignored; (e.g. a transmission radius of three hundred meters results in the reception of BSMs from many vehicles that do not pose a threat). Without message authentication, every BSM received must be trusted to contain factual

information. In an ideal environment without malice this condition is acceptable. Since malice must be accounted for, a mechanism must be implemented to recognize counterfeit messages which is one of the major concerns in the safety-critical environment of V2V.

Vehicle-resident devices such as LiDAR offer many similar applications that are also available through V2V communication. V2V does not strive to replace this technology as LiDAR allows for functionality unavailable from V2V such as lane departure recognition and non-V2V equipped hazard alerts such as nearby wildlife. These technologies used in conjunction can be utilized to cross verify one another. When a vehicle receives a BSM which alerts the driver of a collision the vehicle-resident devices can confirm the alert. Or, if the BSM was spoofed or modified in transit the vehicle-resident devices can reject the V2V application alert and notify the driver. Many consumer vehicles can be purchased today with vehicle-resident technology thus by the time V2V is available most vehicles will have this technology standard.

5.5 Future Work

This thesis focused on BSM linking between vehicles in SCMS, VBSS, and VBSS-D PKI schemes. However, the scope of this thesis was limited. In simulation, only one Road Side Unit (RSU) was utilized along with only five vehicles in effort to emphasize the linking of pseudonyms before and after rotation. In future, more RSUs and more vehicles could be added to show that complete patterns of life can be determined regardless of simulation size. In addition, with the procurement of V2V and LiDAR devices, the viability of cross-platform message verification can be analyzed.

5.6 Conclusion

The benefits of V2V communication have the potential to greatly improve traffic safety, congestion, and environmental conditions – likely greater than the inclusion of any other vehicular safety mechanism. This thesis described how safety and privacy are two opposing perspectives where totality in one meant degradation of the other. The nefarious motives and resources of third party BSM collectors should not be underestimated. The risk mitigation of BSM linking will never be completely reduced as long as vehicles transmit precise location data. However, incorporating methods such as dithering and group-based pseudonyms could increase the sophistication necessary for eavesdroppers to perform BSM linking. Finally, this document questioned the necessity of message authentication and proposed the use of technology such as LiDAR in conjunction with V2V communication to verify message contents.

Data ambiguity methods – such as dithering – are one way to preserve consumer privacy and retain the safety benefits that VANET technology provides. As more and more vehicles are produced with Vehicle-to-Anything (V2X) communication more sophisticated data ambiguity methods will be developed to protect consumers from malicious actors.

It should also be stated that V2V deployment should not be delayed until every issue is accounted for and mitigated. Rather, staggered deployments in fields where privacy is of no concern would likely increase consumer adoption of V2V. For example, ride-sharing, parcel delivery, and other similar delivery services could benefit from V2V data analytics.

Bibliography

1. National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT), "Federal Motor Vehicle Safety Standards; V2V Communications," 2017.

2. "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," *IEEE Std. 1609*, 2014.

3. R. Posten and C. W. Barrett, "NHTSA Privacy Impact Assessment," Tech. Rep., 2016.

4. T. Derenge, "FCC Allocates Spectrum 5.9 GHz Range for Intelligent Transportation Systems Uses," Accessed: 16-June-2017. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/DOC-177370A1.pdf

5. R. A. Uzcátegui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Communications magazine*, vol. 47, no. 5, 2009.

6. D. Jiang and L. Delgrossi, "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE.* IEEE, 2008, pp. 2036–2040.

7. L. Miao, K. Djouani, B. J. van Wyk, and Y. Hamam, "Evaluation and enhancement of ieee 802.11 p standard: A survey," *Mobile Computing*, vol. 1, no. 1, pp. 15–30, 2012.

8. "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Multi-Channel Operation IEEE Vehicular Technology Society IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Multi-Channel Operation," *IEEE Std. 1609.4-2016*, 2016.

9. Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC multi-channel operations and its implications on vehicle safety communications," in *Vehicular Networking Conference (VNC), 2009 IEEE.* IEEE, 2009, pp. 1–8.

10. "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," *IEEE Std. 1609.2-2016*, 2016.

11. SAE, "Dedicated Short Range Communications (DSRC) Message Set Dictionary," *Surface Vehicle Standard J2735*, 2016.

12. SAE, "On-Board System Requirements for V2V Safety Communications," *Surface Vehicle Standard J2945/1*, 2016.

13. SAE, "Vulnerable Road User Safety Message Minimum Performance Requirements," *Surface Vehicle Recommended Practice J2945/9*, 2017.

14. M. Pina. U.S. Department of Transportation (USDOT) ITS Joint Program Office (ITS JPO). Accessed: 16-Aug-2017. [Online]. Available: https://www.its.dot.gov/factsheets/ITSJPO_overview.htm

15. J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*. Springer, 2002, pp. 251–260.

16. J. Grover, M. S. Gaur, and V. Laxmi, "A novel defense mechanism against sybil attacks in vanet," in *Proceedings of the 3rd international conference on Security of information and networks*. ACM, 2010, pp. 249–255.

17. C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2006, pp. 266–279.

18. Y. Zhang and G. Cao, "V-pada: Vehicle-platoon-aware data access in vanets," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 5, pp. 2326–2339, 2011.

19. H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications*, vol. 16, no. 4, 2009.

20. W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *Vehicular Networking Conference (VNC), 2013 IEEE*. IEEE, 2013, pp. 1–8.

21. D. O'Brien, "Significant security challenge for new vehicle communication standard — Symantec Connect Community," 2014, Accessed: 2017-Nov-04. [Online]. Available: https://www.symantec.com/connect/blogs/significant-security-challenge-new-vehicle-communication-standard

22. J. M. Carter and N. R. Paul, "Analysis of vehicle-based security operations," Oak Ridge National Laboratory (ORNL), Oak Ridge, TN (United States), Tech. Rep., 2015.

23. D. Bezzina and J. Sayer, "Safety pilot model deployment: Test conductor team report," Tech. Rep., 2014.

24. L. Reyzin, A. Lysyanskaya, V. Shmatikov, and A. Smith, "Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0126)," Tech. Rep., 2017.

25. MITRE, "Technical Memorandum : Modeling and Simulation of Areas of Potential V2V Privacy Risk," Tech. Rep., 2016.

26. K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," Washington Univ Seattle Dept Of Electrical Engineering, Tech. Rep., 2005.

27. M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in vanets," in *Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,*. IEEE, 2008, pp. 508–513.

28. F. A. Administration. Automatic Dependent SurveillanceBroadcast. Accessed: 18-Feb-2018. [Online]. Available: {https://www.faa.gov/nextgen/where_we_are_now/nextgen_update/progress_and_plans/adsb/}

29. B. Prince. Air Traffic Control Systems Vulnerabilities Could Make for Unfriendly Skies [Black Hat]. Accessed: 18-Feb-2018. [Online]. Available: {https://www.securityweek.com/air-traffic-control-systems-vulnerabilities-could-make-unfriendly-skies-black-hat}

30. D. J. Solove, "Conceptualizing privacy," pp. 1087–1155, 2002.

31. Merriam-Webster, "Dither," Accessed: 19-Nov-2017. [Online]. Available: https://www.merriam-webster.com/dictionary/dither

32. Team SimPY, "Overview SimPy 3.0.10 Documentation," 2016, Accessed: 2017-Nov-19. [Online]. Available: https://simpy.readthedocs.io/en/latest/

33. P. Golle and K. Partridge, "On the anonymity of home/work location pairs," *Pervasive computing*, pp. 390–397, 2009.

34. S. Hanford, "Common vulnerability scoring system, v3 developement update," in *Forum of Incident and Security Teams (FIRST)*, 2013.

35. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 447–462.

36. e. a. Harding, John, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," Tech. Rep., 2014, Accessed: 2017-Nov-18. [Online]. Available: http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf

37. A. Davies. Waymo Has Taken The Human Out Of Self-Driving Cars. Accessed: 15-Nov-2017. [Online]. Available: https://www.wired.com/story/waymo-google-arizona-phoenix-driverless-self-driving-cars/

38. B. Schell. August Schell Engineers and the World's Largest PKI. Accessed: 20-Nov-2017. [Online]. Available: {https://augustschell.com/august-schell-engineers-pki/}

39. Chip Allocation Technical Workgroup, "Common Access Card Release 1.0 ICC Requirements," Tech. Rep., 2001, Accessed: 18-Nov-2017. [Online]. Available: {https://www.dmdc.osd.mil/smartcard/images/CACRelease1ICCRequirementsv1.pdf}

40. B. Eckfeldt, "What does RFID do for the consumer?" *Communications of the ACM*, vol. 48, no. 9, pp. 77–79, 2005.

41. Electronic Frontier Foundation. Automated License Plate Readers (ALPRs). Accessed: 16-Dec-2017. [Online]. Available: {https://www.eff.org/pages/automated-license-plate-readers-alpr.}

42. R. Price. "Google may be quietly tracking everywhere you go here's how to turn it off". Accessed: 16-Dec-2017. [Online]. Available: http://www.businessinsider.com/google-location-history-maps-everywhere-you-go-how-to-turn-it-off-2017-4

43. C. Adams and S. Lloyd, *Understanding public-key infrastructure: concepts, standards, and deployment considerations.* Sams Publishing, 1999.

44. L. Tien, J. Williams, S. Schoen, and R. Shoemaker, "Before the Department of Transportation National Highway Traffic and Safety Administration (NHTSA) NPRM: Federal Motor Vehicle Safety Standards; V2V Communications," Electronic Frontier Foundation, Tech. Rep., 2017.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
22–03–2018	Master's Thesis	August 2016 — March 2018

4. TITLE AND SUBTITLE

Assessing the Competing Characteristics of Privacy and Safety within Vehicular Ad Hoc Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Connors, Jacob W., GS-11

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-18-M-019

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

intentionally left blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The introduction of Vehicle-to-Vehicle (V2V) communication has the promise of decreasing vehicle collisions, congestion, and emissions. However, this technology will place safety and privacy at odds. The NHTSA has proposed the SCMS as the back end infrastructure for maintaining, distributing, and revoking vehicle certificates attached to every BSM. This Public Key Infrastructure (PKI) scheme is designed around the philosophy of maintaining user privacy through the separation of functions to prevent any one subcomponent from identifying users. However, because of the high precision of the data elements within each message this design cannot prevent large scale third-party BSM collection and pseudonym linking resulting in privacy loss. In response to this difficulty, this document illustrates the fundamental tension between privacy and safety and proposes a data ambiguity method to bridge these concepts within the context of interconnected vehicles. The objective in doing so is to preserve both V2V safety applications and consumer privacy. A VANET Metric Classification is introduced that explores five fundamental pillars of VANETs.

15. SUBJECT TERMS

Vehicular Ad Hoc Network, Vehicle-to-Vehicle, Basic Safety Message, Safety, Privacy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Scott Graham, AFIT/ENG
U	U	U	U	102	19b. TELEPHONE NUMBER *(include area code)* (937) 255-6565, x4581; scott.graham@afit.edu